序

本书是将要出版的一部分为三卷总名叫做“抽象代数学”的卷 1. 这三卷书是以著者过去十年間在北加路里那（North Carolina）大学，約翰·霍帕京（Johns Hopkins）大学及耶鲁（Yale）大学的講义为基础写出的. 总的計划是：本卷作为抽象代数学的导引，敍述最重要的代数概念. 为达到这样的目的，势必不能把所要介紹的論題都作广泛深入的說明；但是仍企图越出代数系的基础理論与初等性质的范围，因此在內容上必須作一定程度的取舍. 我們认为：在这一阶段里，与其貪着表面上多懂一些，不如在若干論題上多深入了解一些.

本书的卷 2，卷 3 較具专門性质，对于其中的論題将作概括的說明. 卷 2 以綫性代数学为主題，敍述向量空間的理論. 卷 3 是域論与加罗华（Galois）的理論，討論域的代数結构与域的賦值.

全书三卷都按課堂用的教本来設計的，包括有大量难易程度不等的习题；若干附有星号的习題是被认为在处理中比較棘手的难題. 少数附有星号的节目（記法如 *1）則表明可以略去，而不致影响对后面內容的理解.

在編写本卷过程中，許多朋友曾提供有益的意見与鼓励. 克里福得（A. H. Clifford），霍契才得（G. Hochschild）与約翰孙（R. E. Johnson）三位教授，芬克拜納（D. F. Finkbeiner）与米尔斯（W. H. Mills）两位博士曾閱过底稿的各部分，对修改原稿提出有益的見解；后面两位还协助校对，在这里謹向他們致以誠恳的謝意.

賈柯勃遜（N. Jacobson）

New Haven, Conn.

1951 年元月 22 日

目　　录

引 論

从集合論来的概念. 自然数系

本册的目的是介紹基本代数系：羣、环、域、带算子羣、模及格．这些代数系的研究包含古典代数学的主要部分；故从这一角度来說，題材是古老的，但这里采用公理开发，方法上較为新穎．因为我們的討論不限于特殊代数系（例如，实数系），初学者有时会为抽象所苦；但通过习題与例子的补充学习，会有助于困难的克服．无論如何，这样做法显然可以节省許多时間，且使訒識更加清楚．

我們将要討論的代数系的基本要素是集合及这些集合的映照．故在叙述中常遇見从集合論引来的概念．所以着手討論代数系之前，有必要在这引論的开端簡单地把这些概念說明一下．我們不打算在这集合論大綱的提要里作严格的叙述，讀者可参考系統而詳細討論这門学問的其他标准教本，其中以布巴基（Bourbaki）的"集合論"（Théorie des Ensembles）特别适合要求．

本引論的第二部分把自然数系 P 作为抽象算系予以概述．以假定能适合皮阿罗（Peano）公理的一个集合及这集合里的映照（后継映照）为出发点．由此，在 P 里导入加法、乘法及次序关系．还把整数系 I 定义为自然数系 P 的一种拓广．最后，引出初等羣論上不可少的关于 I 的一二算术事实．关于自然数系基础理論的完整叙述可参考兰道（Landau）的"分析基础"（Grundlagen der Analysis）及格拉甫斯（Graves）的"实变函数論"（Theory of Functions of Real Variables）．

1. 集合的运算 我們以簡单涉猎集合論的基本概念作为討論的开端．

設 S 是元素 $a, b, c, \cdots$ 的一个任意集合，各元素的本质如

何，与討論无关．我們以 $a \in S$ 或 $S \ni a$ 表示元素 a 属于 S．設 A 与 B 为 S 的两个子集合，如果 A 里每个元素 a 都属于 B，就説 A 含于 B，或 B 含有 A（記法是 $A \subseteq B$，或 $B \supseteq A$）．因此 $A = B$ 的意义是：$A \supseteq B$，同时也有 $B \supseteq A$．如果 $A \supseteq B$，但 $B \neq A$，就記作 $A \supset B$；这时我們説，A 眞的含有 B，或説 B 是 A 的眞子集合．

設 A 与 B 是 S 的任意两个子集合，則同时有 $c \in A$，$c \in B$ 的所有元素 c 的集合叫做 A 与 B 的交，記作 $A \cap B$；推广这意义就可定义任意有限个集合的交．設以 $\{A\}$ 表示由 S 的子集合組成的任一集合，我們可进一步推广而把同时属于 $\{A\}$ 里每个 A 的所有元素 c 的集合定义为交 $\cap A$．如果 $\{A\}$ 为有限集合，以 $A_1, A_2, \cdots, A_n$ 表示时，則交可記为 $\bigcap_1^n A_i$，或 $A_1 \cap A_2 \cap \cdots \cap A_n$．

类似的説明可施于 S 的子集合的邏輯和．由若干子集合 A 組成的集合 $\{A\}$ 的邏輯和或併集是元素 u 的集合，这里 u 至少属于 $\{A\}$ 的某一个 A 里．这集合記作 $\cup A$．如果 $\{A\}$ 为有限集合，則这集合記作 $\bigcup_1^n A_i$，或 $A_1 \cup A_2 \cup \cdots \cup A_n$．

由 S 的所有子集合构成的集合記作 $P(S)$．为着免除例外情形的考虑，有必要把全集合 S 及空集合也作为 $P(S)$ 的成分．空集合可看作零元素，附加于"实有的"子集合所构成的集合里，并記作 ϕ．設 A 与 B 不相交，亦即沒有公共元素时，可用方程 $A \cap B = \phi$ 来表达，这就显出导入空集合的好处．設 S 是 n 个元素的有限集合，則 $P(S)$ 的元素是：空集合 ϕ，各含一个元素的 n 个集合，…，各含有 i 个元素的 $\binom{n}{i} = \frac{n(n-1)\cdots(n-i+1)}{1\cdot 2\cdots i}$ 个集合等等．故 $P(S)$ 里元素的总数是

$$1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = (1+1)^n = 2^n.$$

2. 积集合，映照 設 S 与 T 是任意集合，則积集合 $S \times T$ 是 (s, t) 的集合，这里 $s \in S$，$t \in T$．S 与 T 无須为不同的集合．积集合 $S \times T$ 里的元素 (s, t) 与 (s', t') 作为相等，必須而且只須 $s =$

s', $t = t'$. 設 S 含有 m 个元素 $s_1, s_2, \cdots, s_m$, 而 T 含有 n 个元素 $t_1, t_2, \cdots, t_n$, 則 $S \times T$ 含有 mn 个元素 (s_i, t_j). 一般說来, 設 $S_1, S_2, \cdots, S_r$ 为任意集合, 則 ΠS_i 或 $S_1 \times S_2 \times \cdots \times S_r$ 是 r-維組 $(s_1, s_2, \cdots, s_r)$ 的集合, 这里第 i 个支量 s_i 属于 S_i.

集合 S 到集合 T 內的 (单值) 映照 α 是把每个 $s \in S$ 与一个 $t \in T$ 联系起来的一个对应. s 在 T 里的象, 初等数学上常記做 $\alpha(s)$; 但我們将发現以 $s\alpha$ 或 s^{α} 来表示更为方便. 有了映照 α, 就可得出由 $(s, s\alpha)$ 构成的 $S \times T$ 的子集合, 叫做 α 的图示. 它的特性是:

1. 設 s 是 S 的任一个元素, 則图示里有如 (s, t) 形的一个元素存在.

2. 設 (s, t_1) 与 (s, t_2) 同在图示內, 則 $t_1 = t_2$.

映照 α 能使每个 $t \in T$ 必为某些 $s \in S$ 的象时, 就說 α 是 S 到 T 上的映照. 不論 α 是 S 到 T 內或到 T 上的映照, S 的象集合(即象元素的集合)都記做 $S\alpha$ 或 S^{α}. 設 S 到 T 內的映照 α 使 S 里不同元素的象也不相同, 亦即只有 $s_1 = s_2$, 才有 $s_1\alpha = s_2\alpha$ 时, 这样的 α 称为 1—1 映照. 今設 α 是 S 到 T 上的 1—1 映照, 如果 t 是 T 的任一个元素, 則在 S 里必有唯一元素 s 使 $s\alpha = t$. 故若把这个元素 s 与 t 联系起来, 即得 T 到 S 內的一个映照, 叫做 α 的逆映照, 記作 α^{-1}. 显然 α^{-1} 是 T 到 S 上的 1—1 映照.

S 到 T 內的两个映照 α 与 β 作为相等的充要条件无疑地是: 对于 S 里所有 s, $s\alpha = s\beta$. 这就是說, $\alpha = \beta$ 的充要条件是: 它們有同一的图示.

設 α 是 S 到 T 內的映照, 而 β 是 T 到第三集合 U 內的映照, 則 S 的元素 s 到 U 內元素 $(s\alpha)\beta$ 的映照叫做 α 与 β 的积, 記作 $\alpha\beta$; 故由定义得 $s(\alpha\beta) = (s\alpha)\beta$.

一个集合到它自身內的映照叫做这集合的变换, 其中含有使 S 里每个元素都不动的恆等映照或恆等变换, 記作 1 (必要时或記作 1_S). 設 α 是 S 的任一个变换, 显然有 $\alpha 1 = \alpha = 1\alpha$.

設 α 是 S 到 T 上的 1—1 映照, 而 α^{-1} 是它的逆映照, 則 $\alpha\alpha^{-1} =$

1_S, 而 $\alpha^{-1}\alpha = 1_T$. 反过来說，設 α 是 S 到 T 內的一个映照，而 β 是 T 到 S 內的一个映照，如果 $\alpha\beta = 1_S$, 而 $\beta\alpha = 1_T$, 則 α 与 β 都是 1—1 映照，α 必定是 S 到 T 上的映照，β 必定是 T 到 S 上的映照，而且 $\beta = \alpha^{-1}$. 这性质很有用，并且也容易証明的[1].

积集合的概念使我們能够定义二或多变数的函数的概念. 譬如，函数值属于 T 的 S 里两个变数的函数便是 $S \times S$ 到 T 內的一个映照. 更进一步还可考究 $S_1 \times S_2$ 到 T 內的映照. 但特别饒有趣味的却是 $S \times S$ 到 S 內的映照，这映照叫做 S 里的二元合成.

3. 等价关系 我們說关系 R 被确定在集合 S 里的意思是指：对于任意有序二維組 (a, b)，这里 a, b 属于集合 S，我們能够决定 a 是否与 b 有这已知关系. 更明确地說，关系可定义为 $S \times S$ 到由两个元素构成的集合內的映照. 我們可取"是"与"非"两字为这两个元素. 于是，如果 $(a, b) \to$ 是（亦即映照于"是"），就說：a 对于 b 有已知的关系，記作 $a\mathrm{R}b$. 如果 $(a, b) \to$ 非，就說：a 对于 b 无已知的关系，記作 $a\not\mathrm{R}b$.

設关系～（代替 R）适合下列条件：

1. $a \sim a$（反身性）.

2. $a \sim b$, 則 $b \sim a$（对称性）.

3. $a \sim b$, 且 $b \sim c$, 則 $a \sim c$（传递性）.

这种关系叫做等价关系.

設取平面上点的集合为 S，并以点 a 与 b 在同一水平綫上来定义 $a \sim b$，这样便得等价关系的例. 設 $a \in S$，显然元素 $b \sim a$ 的集合 $\bar{a}$ 是过点 a 的水平綫. 这些綫的集合給出把 S 分成不相交的

---

1) 設 $s_1\alpha = s_2\alpha$, 因

$$s_1 = s_1 1_S = s_1(\alpha\beta) = (s_1\alpha)\beta = (s_2\alpha)\beta = s_2(\alpha\beta) = s_2 1_S = s_2,$$

故知 α 是 1—1 映照. 同理可証 β 也是 1—1 映照. 次因 $S\alpha \subseteq T$, $T\beta \subseteq S$, 故

$$S = S1_S = S(\alpha\beta) = (S\alpha)\beta \subseteq T\beta \subseteq S.$$

由此可見 $S\alpha = T$, $T\beta = S$; 亦即 α 是 S 到 T 上的映照，β 是 T 到 S 上的映照. 最后，設 t 为 T 的任一元素，因

$$t\alpha^{-1} = (t\alpha^{-1})1_S = (t\alpha^{-1})(\alpha\beta) = ((t\alpha^{-1})\alpha)\beta = (t(\alpha^{-1}\alpha))\beta = (t1_T)\beta = t\beta,$$

故 $\alpha^{-1} = \beta$——譯者注.

子集合的一个分解. 今将指出这现象标志着等价关系.

命 S 为任一个集合,并命~为 S 里任一个等价关系. 設 $a\in S$; 命 $\bar{a}$ 表示能使 $b\sim a$ 的所有元素 b 的集合. 由 1 知 $a\in\bar{a}$. 設 b_1 与 b_2 都属于 $\bar{a}$, 由 2 及 3 知 $b_1\sim b_2$. 故 $\bar{a}$ 为等价元素的一个集合. 不但如此, $\bar{a}$ 还是这类型的最大集合. 这因为,如果任一个元素 c 与 $\bar{a}$ 里某元素 b 等价时,则 $c\in\bar{a}$. 我們把 $\bar{a}$ 叫做由元素 a 决定的(或含有元素 a 的)等价类. 設 $b\in\bar{a}$, 則 $\bar{b}\subseteq\bar{a}$; 于是,由 $\bar{b}$ 的最大性得 $\bar{b}=\bar{a}$. 故得重要的結論: 任意两个等价类或者全同,或者它們的交是空集合. 故不同的等价类的集合給出把 S 分裂为不相交的子集合的一个分解.

反之,假定一个已知的集合 S, 按任一方式被分解为不相交的子集合 $A, B, \cdots$. 如果两个集合 A, B 迭合,就規定 A 的元素 a 与 B 的元素 b 有 $a\sim b$; 按这法則来区别 S 里元素, 則在 S 里便可定义一个等价关系. 显然,这关系具有上列各性質,且由这关系决定的等价类恰是已知的集合 $A, B, \cdots$.

由 S 里一个等价关系决定的等价类的集合 $\bar{S}$ 叫做 S 关于給定关系的商集合. 必須指出, $\bar{S}$ 不是 S 的一个子集合,而是 S 的子集合的集合 $P(S)$ 里一个子集合.

等价关系与映照間有密切联系. 首先,設 S 为一个集合, 而 $\bar{S}$ 是 S 关于一个等价关系的商集合,則得 S 到 $\bar{S}$ 上一个自然映照 ν; 这映照是按从 S 的元素 a 映到由 a 决定的等价类 $\bar{a}$ 来定义的. 显然,它是到 $\bar{S}$ 上的一个映照.

反之, 設已知由一个集合 S 到另一个集合 T 上的任一映照 α, 則可利用 α 来定义一个等价关系; 它的法則是: 如果 $a\alpha=b\alpha$, 則 $a\sim b$. 这样定义显然适合公理 1, 2 及 3. 設 a' 为 T 的元素,而 a 为 S 的元素能使 $a\alpha=a'$ 时, 則等价类 $\bar{a}$ 恰是 S 里能映到 a' 的所有元素的集合. 这集合叫做 a' 的逆象,記作 $\alpha^{-1}(a')$.

今假定~是 S 里任一个等价关系,它的商集合为 $\bar{S}$. 命 α 是 S 到 T 上的一个映照,具有这样的性質: 逆象 $\alpha^{-1}(a')$ 是属于 $\bar{S}$ 的一些集合的邏輯和,这就等价于設: 属于 $\bar{S}$ 的任一个集合必含于某逆象

$a'\alpha^{-1}$ 里. 所以这只意味着：如果 S 里任意两个元素 a, b 有 $a\sim b$ 时，則 $a\alpha = b\alpha$. 因此，法則 $\bar{a} \to a\alpha$ 显然定义了 $\bar{S}$ 到 T 上的一个映照，叫做由給定的映照 α 导出的 $\bar{S}$ 的映照，記作 $\bar{\alpha}$. 由方程 $\bar{a}\bar{\alpha} = a\alpha$ 可看出：原映照等于自然映照 $a \to \bar{a}$ 与映照 $\bar{\alpha}$ 的积，即 $\alpha = \nu\bar{\alpha}$.

把映照分解为这样因子形式在后面极为重要. 在逆象 $\alpha^{-1}(a')$ 的集合与 $\bar{S}$ 重合时特别有用；这因为，此时映照 $\bar{\alpha}$ 是 1—1 的. 故若 $\bar{a}\bar{\alpha} = \bar{b}\bar{\alpha}$, 則 $a\alpha = b\alpha$, 而有 $a\sim b$. 因此 $\bar{a} = \bar{b}$. 故得因子分解 $\alpha = \nu\bar{\alpha}$, 这里 $\bar{\alpha}$ 是 $\bar{S}$ 到 T 上的 1—1 映照，而 ν 是自然映照.

为解释上面的討論，試研究平面 S 到 x–軸 T 上的正射影 π_x. 此时点 a 映到 x–軸上过 a 的垂綫的足. 設 a' 为 x–軸上一点，則 $\pi_x^{-1}(a')$ 为过 a' 的鉛直綫上的点的集合. 逆象的集合即这些鉛直綫的集合，而导出的映照 $\bar{\pi}_x$ 是把鉛直綫映到它与 x–軸的交点. 显然这映照是 1—1 的，且 $\pi_x = \nu\bar{\pi}_x$, 这里 ν 是一点映到含有这点的鉛直綫的自然映照.

4. 自然数 自然数 1, 2, 3, … 成为代数学上基本代数系的理由有二：第一，它作为构成更精緻的代数系的例子的一个出发点. 譬如利用它来造整数系、有理数系、以整数为模的剩余类系等等. 第二，在研究代数系时，自然数集合的函数或映照极为重要. 例如，在定义有結合乘法的代数系里，固定元素 a 的冪 a^n 决定自然数集合的一个函数或映照 $n \to a^n$.

今从关于自然数集合 P 的下列假設（本質上即是皮阿罗 (Peano) 公理）出发[1].

---

1) 皮阿罗关于自然数的公理如次：

(i) 存在有一个自然数 1.

(ii) 每个自然数 a 有一个后継元素 a^+. 如果 a^+ 是 a 的后継元素，則 a 叫做 a^+ 的生成元素.

(iii) 自然数 1 无生成元素.

(iv) 如果 $a^+ = b^+$, 則 $a = b$.

(v) 自然数的每个集合，如果它含有 1, 并且含有集合内每个元素的后継元素，則这集合含有一切自然数.

从皮阿罗公理可推出上面 1—4 各公理. 这因为，由 (i) 知：P 不是空集合. 由 (ii) 及 (iv) 知：映照 $a\to a^+$ 是 1—1 的. 由 (iii) 知：后継元素的映照所得象集合里不

1. P 不是空集合.

2. 有 P 到 P 内的 1—1 映照 $a \to a^+$ 存在 (a^+ 是 a 的直接后継元素).

3. 从后継元素的映照所得象的集合是 P 的眞子集合.

4. 如果 P 的任一个子集合含有非后継元素的元素，并且含有这子集合里每个元素的后継元素，則它必与 P 重合. 这假設叫做归納法公理.

关于 P 要叙述的所有性質都是这些公理的推論. 由 3 及 4 知，如果 P 的任意两个元素都为非后継元素，則必相等. 这唯一的非后継元素通例記作 1. 我們还命 $1^+ = 2, 2^+ = 3$, 等等.

性質 4 是使用归納法第一原理来証題的理論根据. 这原理是：設对于每个自然数 n 附带有命題 $E(n)$. 如果 $E(1)$ 是眞的，并設凡 $E(r)$ 是眞时 $E(r^+)$ 也是眞. 則 $E(n)$ 对于所有 n 都是眞. 这因为，如果以 S 表能使 $E(s)$ 为眞的自然数 s 的集合，則这个集合含有 1，而且 $r \in S$ 时，r^+ 也必属于 S. 故由 4 直接得出 $S = P$；就是說，$E(n)$ 对于 P 里所有 n 都是眞.

习　題　1

1. 求証：对于各个 n 都有 $n^+ \neq n$.

自然数的加法定义为 P 里一种二元合成，它使得关于 x, y 的值 $x + y$ 适合

(a) $$1 + y = y^+,$$

(b) $$x^+ + y = (x + y)^+.$$

含有 1，故为 P 的眞子集合. 由 (iii) 及 (v) 得归納法公理. 反过来，由 1—4 各公理也可推出皮阿罗的公理. 令 P' 为 P 里各元素的后継元素构成的集合. 如果 P 里每个元素总是某个元素的后継元素，則 $P \subseteq P'$；但由 3，这与 $P' \subset P$ 矛盾. 故 P 里含有非后継元素的元素. 令 e 为这样一个元素，則 $e \in P$, $e \notin P'$. 作子集合 $P_1 = \{e, P'\}$. 因 $e \in P_1$，而且 $e^+ \in P'$，又 P' 里每个元素的后継元素也属于 P'；故由 4 知：$P' = P$. 命 e 为 1，这就导出 (i) 及 (iii). 由 2 得 (ii) 及 (iv). 由 4 得出 (v). 故这两組公理是等价的——譯者注.

这样函数不但存在，且为唯一，是可以証明的[1]. 此外，还有下列的基本性质[2]：

1）先证关于給定的 y 与关于每个 x，存在有一个函数 $x+y$，具有性质(a)及(b)令 P_2 是所有这样 y 的集合，对于它們，这种函数是存在的．于是：

① 当 $y=1$ 时，对于任意的 x，令 $x+y=x^+$．则因为

$$1+y=1^+=y^+,\qquad x^++y=(x^+)^+=(x+y)^+,$$

显見这个函数具有所需的性质，故 $1\in P_2$.

② 如果 $y\in P_2$，則 $x+y$ 被确定，而且具有性质(a)及(b)．关于 x，令 $x+y^+=(x+y)^+$，則因为

$$1+y^+=(1+y)^+=(y^+)^+,$$
$$x^++y^+=(x^++y)^+=[(x+y)^+]^+=(x+y^+)^+,$$

显見这个函数关于 y^+ 也具有所需的性质，故 $y^+\in P_2$.

按归納法公理知 $P_2=P$，即关于任何 y 存在着一个函数，使关于每个 x 的函数值是 $x+y$，而且这个函数关于給定的 y 与任意的 x 具有性质(a)及(b)．但 y 是任意的，所以这种函数的存在就被証明了．

今証关于給定的 y 与关于每个 x 所存在具有性质(a)及(b)的函数不能多于一个．

由上段論証知，函数 $x+y$ 对于任何 x 适合

$$1+y=y^+,\qquad x^++y=(x+y)^+,$$

今設函数 $x\oplus y$ 关于任何 x 也具有

$$1\oplus y=y^+,\qquad x^+\oplus y=(x\oplus y)^+.$$

令 P_1 是关于給定的 y 能使 $x+y=x\oplus y$ 的所有 x 的集合．于是：

①因为 $1+y=y^+=1\oplus y$，故 $1\in P_1$.

② 設 $x\in P_1$，則 $x+y=x\oplus y$．由皮阿罗公理(ii)得 $(x+y)^+=(x\oplus y)^+$．所以，

$$x^++y=(x+y)^+=(x\oplus y)^+=x^+\oplus y.$$

故 $x^+\in P_1$．由归納法公理知，$P_1=P$；即对于給定的 y 与任何 x 都有 $x+y=x\oplus y$．但 y 是任意的，故对于任意的 x 及 y，函数的唯一性就被証明了——譯者注．

2）要証 A_1，設 y 与 z 固定，而令适合 A_1 的所有 x 的集合为 P_1．因

$$1+(y+z)=(y+z)^+=y^++z=(1+y)+z,$$

故 $1\in P_1$．次設 $x\in P_1$，則 $x+(y+z)=(x+y)+z$；于是，

$$x^++(y+z)=(x+(y+z))^+$$
$$=((x+y)+z)^+=(x+y)^++z=(x^++y)+z,$$

故在 $x\in P_1$ 时，$x^+\in P_1$．由归納法公理知 $P_1=P$.

要証 A_2，先証 $1+y=y+1$．令适合这等式的所有 y 的集合为 P_2，显然 $1\in P_2$．次設 $y\in P_2$，則 $1+y=y+1$．于是，由 A_1 得

$$1+y^+=1+(1+y)=1+(y+1)=(1+y)+1=y^++1,$$

故 $y^+\in P_2$．由公理 4 知，$P_2=P$.

次令适合 A_2 的所有 x 的集合为 P_1．由上面証明知，$1\in P_1$．今設 $x\in P_1$，則 $x+y=y+x$．于是，由 A_1 得

$$x^++y=(x+y)^+=(y+x)^+=y^++x$$

A_1 $x+(y+z)=(x+y)+z$ (加法結合律),

A_2 $x+y=y+x$ (加法交換律),

A_3 $x+z=y+z$ 可推得 $x=y$ (加法相消律).

这些結果以及下列关于乘法与次序的結果的証明具載于上述教本中,故从略.

P 里乘法也是一种二元合成,适合

(a) $$1y=y,$$

(b) $$x^+y=xy+y.$$

这样合成是存在的,也是唯一的[1],并具有通常性质[2]:

$$=(1+y)+x=(y+1)+x=y+(1+x)=y+x^+,$$

故 $x^+\in P_1$. 由公理4知, $P_1=P$.

要証 A_3, 設适合 A_3 的所有 z 的集合为 P_3. 因为如果 $x+1=y+1$, 則

$$x^+=1+x=x+1=y+1=1+y=y^+,$$

故由皮阿罗公理 (iv) 知, $x=y$. 所以 $1\in P_3$. 次設 $z\in P_3$, 則 $x+z=y+z$ 时, $x=y$. 于是,当 $x+z^+=y+z^+$ 时,

$$x^++z=(x+z)^+=(z+x)^+=z^++x$$
$$=x+z^+=y+z^+=z^++y=(z+y)^+=(y+z)^+=y^++z,$$

故由归納法假設知, $x^+=y^+$, 由皮阿罗公理 (iv) 知, $x=y$, 于是, $z^+\in P_3$;故 $P_3=P$ ——譯者注.

1) 先証关于給定的 y 与关于每个 x, 存在有一个函数 $x\cdot y$, 具有性质 (a) 及 (b). 令 P_2 是所有这样 y 的集合,对于它們,这种函数是存在的. 于是:

① 当 $y=1$ 时,对于任意的 x, 令 $x\cdot y=x$, 則因为

$$1\cdot y=1=y,\qquad x^+\cdot y=x^+=x+y=x\cdot y+y,$$

显見这个函数具有所需的性质,故 $1\in P_2$.

② 如果 $y\in P_2$, 則 $x\cdot y$ 被确定, 而且具有性质 (a) 及 (b). 关于 x, 令 $x\cdot y^+=xy+x$, 則由 A_1 及 A_2 得:

$$1\cdot y^+=1\cdot y+1=y+1=y^+,$$
$$x^+\cdot y^+=x^+\cdot y+x^+=(x\cdot y+y)+x^+=x\cdot y+(y+x^+)$$
$$=x\cdot y+(y+x)^+=x\cdot y+(x+y)^+=x\cdot y+(x+y^+)$$
$$=(x\cdot y+x)+y^+=x\cdot y^++y^+,$$

显見这个函数关于 y^+ 也具有所需的性质,故 $y^+\in P_2$.

按归納法公理知 $P_2=P$; 即关于任何 y 存在着一个函数, 使关于每个 x 的函数值是 $x\cdot y$, 而且这个函数关于給定的 y 与任意的 x 具有性质 (a) 及 (b). 但 y 是任意的, 所以这种函数的存在就被証明了.

今証关于給定的 y 与关于每个 x 所存在具有性质 (a) 及 (b) 的函数不能多于一个.

由上段論証知,函数 $x\cdot y$ 对于任何 x 适合

$$1\cdot y=y,\qquad x^+\cdot y=x\cdot y+y.$$

(續下頁)

M_1 $x(yz)=(xy)z$ (乘法結合律),

M_2 $xy=yx$ (乘法交换律),

M_3 $xz=yz$ 可推得 $x=y$ (乘法相消律).

此外还有連結加法与乘法的下列基本法則:

D $x(y+z)=xy+xz$ (分配律).

今設函数 $x\odot y$ 关于任何 x 也具有

$$1\odot y=y,\qquad x^+\odot y=x\odot y+y.$$

令 P_1 是关于給定的 y 能使 $x\cdot y=x\odot y$ 的所有 x 的集合,于是,

① 因为 $1\cdot y=y=1\odot y$, 故 $1\in P_1$.

② 設 $x\in P_1$, 則 $x\cdot y=x\odot y$. 故

$$x^+\cdot y=x\cdot y+y=x\odot y+y=x^+\odot y.$$

所以 $x^+\in P_1$. 由归納法公理知, $P_1=P$; 即对于給定的 y 与任何 x 都有 $x\cdot y=x\odot y$. 但 y 是任意的,故对于任意的 x 及 y, 函数 $x\cdot y$ 的唯一性就被証明了——譯者注.

2) 要証 M_1 与 M_2, 我們先証 D. 設 y 与 z 固定,而令适合 D 的所有 x 的集合为 P_1. 因

$$1\cdot(y+z)=y+z=1\cdot y+1\cdot z,$$

故 $1\in P_1$. 次設 $x\in P_1$, 則 $x(y+z)=xy+xz$; 于是,

$$x^+(y+z)=x(y+z)+(y+z)=xy+xz+y+z$$
$$=(xy+y)+(xz+z)=x^+y+x^+z,$$

故 $x^+\in P_1$. 由公理 4 知, $P_1=P$.

今証 M_2. 先証 $1\cdot y=y\cdot 1$. 令适合这等式的所有 y 的集合为 P_2, 显然 $1\in P_2$. 次設 $y\in P_2$, 則 $1\cdot y=y\cdot 1$. 于是,

$$1\cdot y^+=y^+=1+y=y+1=1\cdot y+1=y\cdot 1+1=y^+\cdot 1,$$

故 $y^+\in P_2$. 由公理 4 知, $P_2=P$.

次令适合 M_2 的所有 x 的集合为 P_1. 由上面証明知, $1\in P_1$. 次設 $x\in P_1$, 則 $xy=yx$. 于是

$$x^+y=xy+y=y+xy=y\cdot 1+yx=y(1+x)=yx^+,$$

故 $x^+\in P_1$. 由公理 4 知 $P_1=P$.

要証 M_1, 設 y 与 z 固定,而令适合 M_1 的所有 x 的集合为 P_1. 因

$$1\cdot(yz)=(yz)=(1\cdot y)z,$$

故 $1\in P_1$. 次設 $x\in P_1$, 則 $x(yz)=(xy)z$; 于是由 D 及 M_2 得

$$x^+(yz)=x(yz)+yz=(xy)z+yz$$
$$=z(xy)+zy=z(xy+y)=z(x^+y)=(x^+y)z,$$

故 $x^+\in P_1$. 由公理 4 知, $P_1=P$.

最后,証 M_3. 令适合 M_3 的所有 z 的集合为 P_3. 显然 $1\in P_3$, 这因为, 由 $x\cdot 1=y\cdot 1$, 得

$$x=1\cdot x=x\cdot 1=y\cdot 1=1\cdot y=y.$$

次設 $z\in P_3$, 則由 $xz=yz$ 推得 $x=y$. 于是得

$$xz^+=z^+x=zx+x=xz+x=yz+y=zy+y=z^+y=yz^+.$$

故 $z^+\in P_3$. 由公理 4 知, $P_3=P$——譯者注.

算系 P 的第三个基本概念为**次序**；它的定义可借加法述出．設方程 $a=b+x$ 对于 x 有属于 P 的一个解，我們就說 a 大于 b（記作 $a>b$，或 $b<a$）．这关系的基本性质是[1]：

O_1　$x>y$ 則不能有 $x\leqslant y$（反对称性），

O_2　$x>y$，且 $y>z$，可推得 $x>z$（传递性），

O_3　对于任一个有序二維組 (x,y)，$x>y$，$x=y$，$x<y$ 三者中必居其一（鼎立性）．（O_1 可从这性质推得．这里一起列出是因为有些代数系适合 O_1 与 O_2，但不适合 O_3，而我們对于这样代数系常感兴趣的緣故．）

O_4　在自然数的任一个非空集合里必有一个最小数存在；就是說，对于集合里所有数 s 中存在着一个数 l 使 $l\leqslant s$．

O_4 的証明　命 S 为已知的集合，而 M 为比 S 里各元素 s 小或相等的自然数 m 的集合．則 $1\in M$．設 s 为 S 里一个特殊元素，則 $s^+>s$；于是，$s^+\notin M$．故 $M\neq P$．根据归納法原理，必有一个自然数 l 存在使 $l\in M$，但 $l^+\notin M$．l 就是所求．这因为，如果 l 小于 S 里各个 s，則 $l^+\leqslant s$，这与 $l^+\notin M$ 矛盾．故 $l\leqslant S$ 里各个 s，而且 $l\in S$．

1）因 O_3 可推出 O_1，故只須証 O_3．为着这目的，我們先証：适合 $a=a+u$ 的 a 在 P 中不存在，这里 $u\in P$．首先取 $a=1$，則因 $1=1+u=u^+$ 与皮阿罗公理 (iii) 矛盾，故 1 不适合要求．次設有 a 存在使 $a=a+u$，則

$$a+1=1+a=a^+=(a+u)^+$$
$$=a^++u=(1+a)+u=(a+1)+u=a+(1+u).$$

由 A_3，得 $1=1+u$；这与上面証得的結果矛盾．

今証 O_3．設 $x>y$，則 P 中有数 u 存在，使 $x=y+u$．如果同时更有 $x=y$，則有 $y=y+u$，这与上面証得的結果矛盾，亦即 $x=y$ 不能同时成立．如果同时更有 $x<y$，則 P 中有数 v 存在使 $y=x+v$．于是，

$$y=x+v=(y+u)+v=y+(u+v);$$

这也与上面証得的結果矛盾．故不能同时有 $x<y$．

仿此可証：当 $x=y$ 时，$x>y$ 及 $x<y$ 也不能同时成立；$x<y$ 时 $x>y$ 及 $x=y$ 也不能同时成立．

要証 O_2．由假設 $x>y$，$y>z$，故在 P 中存在有 u 及 v，使 $x=y+u$，$y=z+v$．于是，

$$x=(z+v)+u=z+(v+u);$$

故 $x>z$——譯者注．

性质 O_4 叫做 P 的良序性，是归納法第二原理的理論根据. 这原理是說：設对于每个 $n \in P$，有一个命題 $E(n)$. 如果对于所有 $s < r$, $E(s)$ 都是眞的，就可推知对于特定的 r, $E(r)$ 也是眞时(这里含有已知 $E(1)$ 是眞的)，則 $E(n)$ 对于所有 n 都是眞. 要証这原理，命 F 是使 $E(r)$ 不眞的元素 r 的集合. 如果 F 不为非空集合，命 t 是它的最小元素，則 $E(t)$ 不眞；但对于所有 $s < t$, $E(s)$ 是眞的，这与假設矛盾. 故 F 是空集合，而 $E(n)$ 对于所有 n 都是眞.

次序与加法間及次序与乘法間的主要关系如次[1]：

OA　$a > b$，必須而且只須 $a + c > b + c$.

OM　$a > b$，必須而且只須 $ac > bc$.

习　題　2

1. 設 $a>b$, $c>d$, 求証: $a+c>b+d$, $ac>bd$.

5. 整数系　要获得自然数的拓广代数系，通常办法是于 P 里添入 0 元素及負元素；但这里采取另一办法，似覚更自然而且更直观些. 我們要作整数的新代数系 I，它含有与自然数集合本质相同的一个子代数系.

首先研究自然数的有序二維組 (a, b) 的集合 $P \times P$. 在这集合里引入关系 $(a, b) \sim (c, d)$，它按 $a + d = b + c$ 来决定. 不难証实，这是一个等价关系. 我們作这定义的用意，事实上是把由 (a, b) 决定的等价类 $\overline{(a, b)}$ 来代替 a 与 b 的差. 設按通例，以点表示二維組 (a, b)，a 为它的横坐标，b 为纵坐标. 則 $\overline{(a, b)}$ 是在过 (a, b) 而斜率为 1 的直綫上以自然数做坐标的点的集合.

---

1) 先証 OA 成立. 如果 $a>b$，則 P 中有一数 u 使 $a = b + u$. 于是，

$$a + c = (b + u) + c = b + (u + c) = b + (c + u) = (b + c) + u.$$

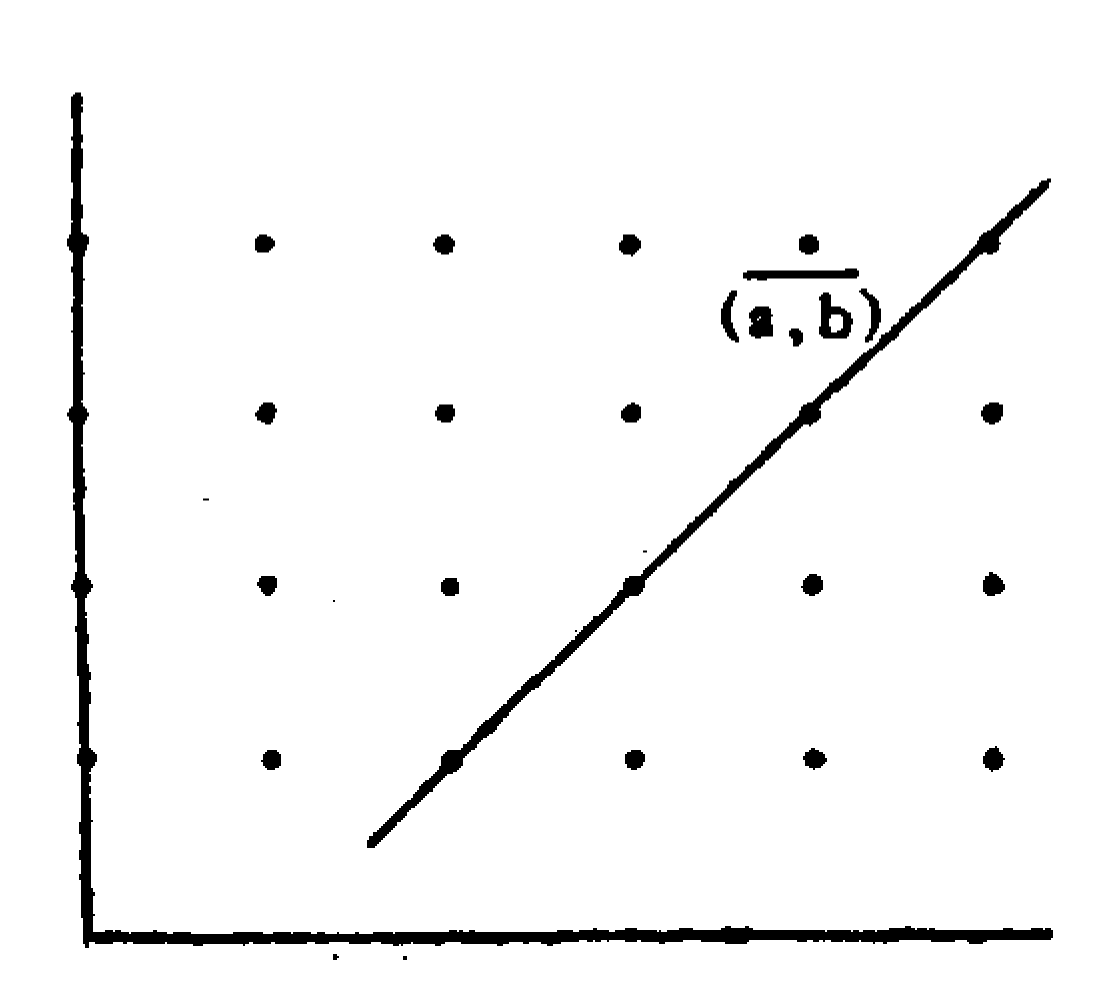
故 $a + c > b + c$. 反过来，如果 $a + c > b + c$，則 P 中有一数 u 使 $a + c = (b+c) + u = b + (c + u) = b + (u + c) = (b + u) + c$. 由 A_8 得 $a = b + u$; 故 $a > b$.

次証 OM 成立. 如果 $a > b$，則 P 中有一数 u 使 $a = b + u$. 于是 $ac=(b + u)c= bc + uc$，故 $ac > bc$. 反过来，如果 $ac > bc$，而 $a = b$，或 $a < b$，則必有 $ac = bc$ 或 $ac < bc$. 但由鼎立性知，这都与假設矛盾，故 $a > b$——譯者注.

我們叫这种等价类做整数，其全体記作 I. 作为定义加法的准备，我們先指出：設

$$(a, b) \sim (a', b'),$$
$$(c, d) \sim (c', d'),$$

则 $(a+c, b+d) \sim (a'+c', b'+d')$.



这因为，由假設得

$$a + b' = a' + b,$$
$$c + d' = c' + d.$$

故 $a + c + b' + d' = a' + c' + b + d$. 这意味着

$$(a + c, b + d) \sim (a' + c', b' + d').$$

故整数 $\overline{(a + c, b + d)}$ 是 $\overline{(a, b)}$ 与 $\overline{(c, d)}$ 的函数；这个整数就定义为整数 $\overline{(a, b)}$ 与 $\overline{(c, d)}$ 的和：

$$\overline{(a, b)} + \overline{(c, d)} = \overline{(a + c, b + d)}.$$

法則 A_1, A_2, A_3 容易証其成立. 我們还可看出，$(a, a) \sim (b, b)$. 設命 $0 = \overline{(a, a)}$，則

A_4 对于 I 内各个 x，有 $0 + x = x$.

最后还可看出，每个整数都有負的. 設 $x = \overline{(a, b)}$，并把 $\overline{(b, a)}$ 記作 $-x$，則有

A_5 $x + (-x) = 0$.

其次，我們可看出，設 $(a, b) \sim (a', b')$, $(c, d) \sim (c', d')$，則 $a + b' = a' + b$, $c + d' = c' + d$. 故

$$c(a + b') + d(a' + b) + a'(c + d') + b'(c' + d)$$
$$= c(a' + b) + d(a + b') + a'(c' + d) + b'(c + d'),$$

于是，

$$ac + b'c + a'd + bd + a'c + a'd' + b'c' + b'd$$
$$= a'c + bc + ad + b'd + a'c' + a'd + b'c + b'd'.$$

由相消律得

$$ac + bd + a'd' + b'c' = bc + ad + a'c' + b'd'.$$

这指出 $(ac + bd, ad + bc) \sim (a'c' + b'd', a'd' + b'c')$. 故若定义

$$\overline{(a, b)}\overline{(c, d)} = \overline{(ac + bd, ad + bc)},$$

則得一个单値函数. 这积函数可証其能适合結合律、交換律及关于加法的分配律. 如果相消去的因子 $z \neq 0$，則相消律也成立[1].

若 $a + d > b + c$，我們就認为整数 $\overline{(a, b)} > \overline{(c, d)}$. 这关系是正确的. O_1, O_2, O_3 及 OA 都容易証其成立[2]；性质 OM 則修

---

1) 由等价类的加法及乘法的定义，直接可証結合律、交換律及分配律是成立的. 这里只証相消律也成立. 令 $x = \overline{(a, b)}$, $y = \overline{(c, d)}$, $z = \overline{(e, f)}$. 因 $z \neq 0$，故 $e \neq f$. 为确定計，設 $e > f$；令 $e = f + u$. 如果 $xz = yz$，則 $\overline{(ae + bf, af + be)} = \overline{(ce + df, cf + de)}$. 所以

$$ae + bf + cf + de = af + be + ce + df,$$
$$(a + d)e + (b + c)f = (a + d)f + (b + c)e,$$

以 $e = f + u$ 代入，得

$$(a + d + b + c)f + (a + d)u = (a + d + b + c)f + (b + c)u.$$

由 A_3 得 $(a + d)u = (b + c)u$. 由 M_8 得 $a + d = b + c$. 故 $\overline{(a, b)} = \overline{(c, d)}$；亦即 $x = y$.

同理可証 $e < f$ 时相消律也成立. ——译者注.

2) 由 P 的鼎立性，立見等价类也具有鼎立性，即 O_3 成立；从而 O_1 也成立.

要証 O_2 成立，設 $\overline{(a, b)} > \overline{(c, d)}$, $\overline{(c, d)} > \overline{(e, f)}$，則由定义有 $a+d > b+c$, $c + f > d + e$. 故由 OA 得

$$(a + f) + d = a + d + f > b + c + f > b + d + e = (b + e) + d.$$

再由 OA 得 $a + f > b + e$. 故 $\overline{(a, b)} > \overline{(e, f)}$.

要証 OA 对于等价类也成立. 命 $x = \overline{(a, b)}$, $y = \overline{(c, d)}$, $z = \overline{(e, f)}$. 設 $x > y$，則 $a + d > b + c$. 由 OA 得

$$(a + d) + (e + f) > (b + c) + (e + f);$$

故

$$(a + e) + (d + f) > (b + f) + (c + e).$$

由定义知，$\overline{(a + e, b + f)} > \overline{(c + e, d + f)}$，亦即 $x + z > y + z$. 反过来，可将上面各步驟倒轉，即得出 $\overline{(a, b)} > \overline{(c, d)}$，亦即 $x > y$.

要証 OM′，命 $x = \overline{(a, b)}$, $y = \overline{(c, d)}$, $z = \overline{(e, f)}$. 因 $z > 0$，故 $e > f$. 令 $e = f + u$. 又因 $x > y$，故 $a + d > b + c$. 由 OM 得 $(a + d)u > (b + c)u$. 由 OA 得

$$(*) \qquad (a + d)u + (a + d + b + c)f > (b + c)u + (a + d + b + c)f.$$

使用 $f + u = e$，得

$$(a + d)e + (b + c)f > (a + d)f + (b + c)e,$$

亦即

$$(ae + bf) + (cf + de) > (af + be) + (ce + df),$$

故 $\overline{(ae + bf, af + be)} > \overline{(ce + df, cf + de)}$，亦即 $xz > yz$. 反过来，如果 $z > 0$，而 $xz > yz$；将上面各步驟倒轉，得到(*)．然后由 OA 得 $(a + d)u > (b + c)u$. 由 OM 得 $a + d > b + c$，故 $\overline{(a, b)} > \overline{(c, d)}$；亦即 $x > y$. ——译者注.

故成

OM′ 設 $z > 0$，則 $x > y$ 必須而且只須 $xz > yz$.

习 题 3

1. 設 $x > y$，求証：$-x < -y$.

今研究正整数的集合 P'. 按定义，这集合是 I 里元素 $x > 0$ 所組成的子集合. 設 $x = \overline{(a, b)}$，則 $x > 0$ 相当于要求 $a > b$. 故 $x = \overline{(b + u, b)}$，且有 $(b + u, b) \sim (c + u, c)$. 命 u 为任一个自然数（P的元素），并定义 u' 为正整数 $\overline{(b + u, b)}$. 由上面討論可見：映照 $u \to u'$ 是 P 到 P' 上的一个单值映照. 此外，如果还有 $(b + u, b) \sim (c + v, c)$，于是 $b + u + c = b + c + v$，必使 $u = v$. 故 $u \to u'$ 为 1—1 映照. 讀者可証这种对应还有下列各性质[1]：

$$(u + v)' = u' + v',$$

$$(uv)' = u'v',$$

$$u > v \text{ 等价于 } u' > v'.$$

故 (1) 先求两自然数的和，然后求这和的对应正整数，或 (2) 先求这两个自然数的对应正整数然后求和，結果都是一样. 乘法方面，类似的說法也是成立的. 因此，原来的自然数系可以废弃，而用正整数系来代替，并可把原来用于 P 的記法即充用为正整数系的記法. 故此后即以 P 表正整数系，它的数就記作 1, 2, 3, …；而 I 里其余各数就記作 0, −1, −2, ….

习 题 4

1. 整数的任一个非空集合 S 为下(上)有界的，其意义是説：对于 S 里各个 s，有一个整数 $b(B)$ 存在，使 $b \leqslant s$ $(B \geqslant s)$. 求証：这样的 S 含有一个最小(最大)元素.

---

1) 令 $u' = \overline{(b + u, b)}$，$v' = \overline{(c + v, c)}$，則

$$(u + v)' = \overline{(b + c + u + v, b + c)} = \overline{(b + u + c + v, b + c)}$$
$$= \overline{(b + u, b)} + \overline{(c + v, c)} = u' + v'.$$
$$(uv)' = \overline{(2bc + bv + cu + uv, 2bc + bv + cu)}$$
$$= \overline{((b + u)(c + v) + bc, (b + u)c + b(c + v))} = u'v'.$$

次設 $u > v$，由 OA 得 $u + b + c > v + b + c$，亦即 $(b+u)+c > b+(c+v)$. 故 $\overline{(b + u, b)} > \overline{(c + v, c)}$；亦即 $u' > v'$. 将各步驟倒轉，就可証：如果 $u' > v'$，則 $u > v$. ——譯者注.

2. 若 $x \geqslant 0$, 则命 $|x| = x$; 但若 $x < 0$, 则命 $|x| = -x$. 求証

$$|xy| = |x||y|, \quad |x+y| \leqslant |x| + |y|.$$

6. 在 I 里的除法 在羣及整区的討論过程中，将得出关于 I 的若干初等的算术性质. I 的算术研究的出发点是下面的熟知結果.

定理 設 a 为任一个整数，而 $b \neq 0$，則有整数 q，r 存在，$0 \leqslant r < |b|$，使 $a = bq + r$.

証 在 $|b|$ 的倍数 $x|b|$ 中考虑 $\leqslant a$ 的那些倍数. 因 $-|a||b| \leqslant -|a| \leqslant a$，可見这些倍数的集合 M 为非空集合；故 M 含有一个最大元素 $h|b|$. 于是，$h|b| \leqslant a$，而 $a = h|b| + r$，这里 $r \geqslant 0$. 次因

$$(h+1)|b| = h|b| + |b| > h|b|,$$

故 $(h+1)|b| > a$，而且 $h|b| + |b| > h|b| + r$；于是，$r < |b|$. 設 $b > 0$ 时取 $q = h$，而在 $b < 0$ 时取 $q = -h$，則 $h|b| = qb$，而 $a = qb + r$，即为求証結果.

习　题　5

1. 求証：q 与 r 是唯一的.

設对于整数 a 与 b，有一个整数 c 存在，使 $a = bc$，則 b 叫做 a 的因子或除数，而 a 叫做 b 的倍数. 这关系記作 $b|a$. 显然这是一种传递关系. 設 $b|a$，且 $a|b$，則有 $a = bc$，$b = ad$；于是，$a = adc$. 設 $a \neq 0$，由相消律可推得 $dc = 1$. 故 $|d||c| = 1$，而得 $d = \pm 1$，$c = \pm 1$. 这指出：如果 $b|a$，且 $a|b$ 而 $a \neq 0$，則 $a = \pm b$.

設 a, b, d 为整数，(1) 設 $d|a$，且 $d|b$，(2) 設 e 为 a 与 b 的任一个公因子时，則 $e|d$；具有这两个性质的 d 叫做 a 与 b 的最大公因子(記号为 g. c. d.). 当 $a \neq 0$ 时，任两个整数 a, b 有一个最大公因子存在，可由上面关于除法的定理容易証出. 欲实現这目的，考究 $ax + by$ 形的整数的全体 D. 这集合含有正整数，故必含有一个最小正整数 $d = at + bs$. 令 $a = dq + r$，則 $0 \leqslant r < d$. 又因

$$r = a - dq = a(1 - qt) + b(-qs) \in D.$$

而 d 是 D 里最小正整数，故必 $r = 0$，亦即 $d|a$. 同理知 $d|b$. 次命 $e|a$ 且 $e|b$，則 $e|at$，$e|bs$；于是 $e|(at + bs)$，亦即 $e|d$.

設 d' 为 a 与 b 的另一个最大公因子，由 (2) 推得 $d|d'$ 及 $d'|d$，故 $d' = \pm d$. 于是，我們常可取 $d \geqslant 0$；这个特殊的最大公因子此后記作 (a, b).

如果整数 p 只能为 p，$-p$，1，-1 所除尽，p 就叫做素数. 最大公因子的存在提供算术的基本定理的証明以理論根据. 这定理是：任一个正整数可以正素数的积表出，而且表达是唯一的. 后面(第四章)我們討論整区的算术性质时就得到这結果.

設 m 为整数 a 与 b 的倍数，而 a 与 b 的任一个公倍数都是 m 的倍数时，这 m 叫做 a 与 b 的最小公倍数. 由利用基本定理或最大公因子的簡单性质，我們还可容易証明：整数

$$m = ab/(a, b)$$

是 a 与 b 的最小公倍数.

第 一 章

半 羣 及 羣

羣論是抽象代数学里发达最早而内容最丰富的一个部門. 变換羣在几何学里充重要角色, 而有限羣是加罗华在方程式論上发明的基础. 这两个領域提供羣論发展以原动力.

比羣更普遍的概念是半羣. 这个概念虽在許多場合很有用, 但它的理論比較新;可以肯定地說,它还不能被看做已經达到齐全的阶段. 本章由这个更普遍概念开端, 但只作了簡单的說明. 我們考虑半羣的目的是作为介紹羣論的准备, 以及得出环的研究中要用到的一些初等結果; 論述的主要部分还是羣. 本章所考虑的主要概念有同构、同态、子羣、不变子羣、商羣及变換羣.

1. 半羣的定义及例 集合 $\mathfrak{S}$ 里的二元合成曾定义为积集合 $\mathfrak{S} \times \mathfrak{S}$ 到集合 $\mathfrak{S}$ 内的一个映照. $\mathfrak{S} \times \mathfrak{S}$ 里二維組 (a, b) 在 $\mathfrak{S}$ 内的象常叫做 a 与 b 的积或和, 因此这結果就記作 $a \cdot b \equiv ab$, 或 $a + b$, 别样記法如 $a \cdot b$, $a \times b$, $[a, b]$ 也偶然用到. 本书几乎只討論結合的二元合成, 即对于 $\mathfrak{S}$ 里所有 a, b, c,

$$(ab)c = a(bc) \tag{1}$$

成立. 这概念在将要定义的代数系里是必須的要素.

定义 1. 半羣是由一个集合 $\mathfrak{S}$ 及 $\mathfrak{S}$ 里一个結合的二元合成所組織的代数系.

要叙述一个特殊半羣, 不但要把集合 $\mathfrak{S}$ 指出, 同时还得把作用于 $\mathfrak{S}$ 的二元合成講明; 这因为許多不同的半羣关于集合部分可以是同一的集合. 但为簡单起見, 集合 $\mathfrak{S}$ 常叫做"半羣 $\mathfrak{S}$"; 严格地說, 当然应該叫做 "半羣的集合 $\mathfrak{S}$", 然而在大多数例子上使用略語并无可以产生混淆之处.

例. (1) 正整数的集合 P, 及 P 里普通加法的二元合成. (2) P 及普通乘法. (3) P 及二元合成

$$(a, b) \to a \cdot b \equiv a + b + ab.$$

我們可証它是可結合的. (4) 整数的集合 I, 二元合成是加法. (5) I 及乘法. (6) 由集合 S 的子集合組成的集合 $P(S)$, 二元合成是併集 $(A, B) \to A \cup B$. (7) $P(S)$, 二元合成是交.

半羣的一个重要类型可从給定集合 S 的变换(单值映照)的全体 $\mathfrak{T}$ 得出. 于 $\mathfrak{T}$ 里导入映照 $(\alpha,\beta) \longrightarrow \alpha\beta$, 这里 $\alpha\beta$ 表示变换 α 与 β 的积. 我們必須証結合律能够成立. 本着这目的, 今就四个集合 S, T, U 及 V 这种普遍情况来討論. 令 α 是 S 到 T 內的映照, β 是 T 到 U 內的映照, γ 是 U 到 V 內的映照, 則可确定映照 $(\alpha\beta)\gamma$ 与 $\alpha(\beta\gamma)$. 要証这两个映照相等, 設 x 为 S 的任一个元素, 由定义得

$$x((\alpha\beta)\gamma) = (x(\alpha\beta))\gamma = ((x\alpha)\beta)\gamma,$$
$$x(\alpha(\beta\gamma)) = (x\alpha)(\beta\gamma) = ((x\alpha)\beta)\gamma.$$

故对于所有 x, $x((\alpha\beta)\gamma) = x(\alpha(\beta\gamma))$; 也就是說, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$. 特别是仅就集合 S 的变换的积来說, 結合律当然也是成立.

作为这类型的半羣的特种形态, 命 S 是含有 n 个元素的有限集合, 我們可取整数 $1, 2, \cdots, n$ 为元素. 于是, 映照 α 可記为

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1\alpha & 2\alpha & 3\alpha & \cdots & n\alpha \end{pmatrix}, \qquad (2)$$

k 的象 k_α 在这里是写在元素 k 的下方. S 到它自身內的映照的个数显然等于 (2) 中第二行上不同写法的个数. 因第二行上每个位置都有 n 种选择, 故 $\mathfrak{T}$ 里元素的阶, 或个数, 为 n^n.

設半羣只含有限个元素, 就叫做**有限半羣**. 要討論这样的半羣, 将 $\mathfrak{S}$ 里的积 $\alpha\beta$ 列成**乘法表**是有用的. 設 $\alpha_1, \alpha_2, \cdots, \alpha_m$ 是 $\mathfrak{S}$ 的元素, 則乘法表的形状是

	α_1	α_2	$\cdots$	α_j	$\cdots$	α_m
α_1				$\cdot$		
α_2				$\cdot$		
$\vdots$				$\vdots$		
α_i	$\cdot$	$\cdot$	$\cdots$	$\alpha_i\alpha_j$	$\cdots$	$\cdot$
$\vdots$				$\vdots$		
α_m				$\cdot$		

我們把积 $\alpha_i\alpha_j$ 写在 α_i 的所在行与 α_j 的所在列的交点处. 例如, 命 $\mathfrak{T}$ 是由含有两个元素的集合里所有变换构成的半羣, 則 $\mathfrak{T}$ 的元素是

$$\varepsilon=\begin{pmatrix}1&2\\1&2\end{pmatrix},\quad \alpha=\begin{pmatrix}1&2\\2&1\end{pmatrix},\quad \beta=\begin{pmatrix}1&2\\1&1\end{pmatrix},\quad \gamma=\begin{pmatrix}1&2\\2&2\end{pmatrix};$$

而 $\mathfrak{T}$ 的乘法表是

	ε	α	β	γ
ε	ε	α	β	γ
α	α	ε	β	γ
β	β	γ	β	γ
γ	γ	β	β	γ

2. 非結合的二元合成 我們暫考慮 $\mathfrak{S}$ 里任意(不必为結合的)二元合成 $(a, b) \to ab$. 这样的映照可确定两个三元合成, 亦即 $\mathfrak{S}\times\mathfrak{S}\times\mathfrak{S}$ 到 $\mathfrak{S}$ 内的映照: $(a, b, c) \to (ab)c$ 及 $(a, b, c) \to a(bc)$. 更普遍地說, 在 $\mathfrak{S}$ 里可采取归納方式定义出一批 n 元合成. 設从二元合成起, 已能作出各个 m $(<n)$ 元合成; 我們把 $m=1$ 的一元合成当作是恆等映照 $a\to a$. 今令 m 为 $<n$ 的任一个正整数,幷令

$$(a_1,a_2,\cdots,a_m)\to u(a_1,a_2,\cdots,a_m),$$
$$(a_{m+1},a_{m+2},\cdots,a_n)\to v(a_{m+1},a_{m+2},\cdots,a_n)$$

是由原来二元合成决定出来的某个 m 元与 $(n-m)$ 元合成. 則我們可取

$$(a_1, a_2, \cdots, a_n)\to u(a_1, a_2, \cdots, a_m)v(a_{m+1}, a_{m+2}, \cdots, a_n)$$

为 n 元合成的一个. 随着 m, u, v 的改变,按这方法得出的所有映照都是与 $(a, b)\to ab$ 連帯的 n 元合成. 应用这些映照于 $(a_1, a_2, \cdots, a_n)$ 的結果叫做 $a_1, a_2, \cdots, a_n$ (按这样次序)的(复合)积.

例如, a_1, a_2, a_3, a_4 可能的积有

$$((a_1a_2)a_3)a_4,\qquad (a_1(a_2a_3))a_4,\qquad (a_1a_2)(a_3a_4),$$

$$a_1(a_2(a_3a_4)), \qquad a_1((a_2a_3)a_4).$$

不难作出一个具有二元合成的集合，使得由这二元合成所导出的所有 n 元合成皆不相同．本着这目的，命 S 为不同元素 $a_1, a_2, a_3, \cdots$ 的集合，而 $\mathfrak{S}^*$ 是根据下面方法得出的記号的集合．于 S 里选取任一个有限集合，其元素按一定次序記作 $a, b, \cdots, s$. 如果这集合只有一个或两个元素，就把它归到 $\mathfrak{S}^*$ 里．如果有两个以上的元素，就把它分成两个有序子集合 $a, b, \cdots, k$ 与 $l, \cdots, s$；在这样得来的子集合里所含元素不只一个时，就把它放在括号里，而得 $(a, b, \cdots, k)\ (l, \cdots, s)$．然后再就这两个子集合重复使用上述方法，直到最后为止．設 u 及 v 表示 $\mathfrak{S}^*$ 里任意两个記号，

$$\left.\begin{array}{l}\text{在 } u \text{ 与 } v \text{ 都属于 } S \text{ 时，}\\ \text{在 } u\in S\text{，而 } v \text{ 含有多于一个元素时，}\\ \text{在 } v\in S\text{，而 } u \text{ 含有多于一个元素时，}\\ u \text{ 及 } v \text{ 都含有多于一个元素时，}\end{array}\right\}\text{定义 } uv=\left\{\begin{array}{l}uv,\\ u(v),\\ (u)v,\\ (u)(v).\end{array}\right.$$

显然这在 $\mathfrak{S}^*$ 里給出一个二元合成．且因前此定义的 n 元合成对于元素 $a_1, a_2, \cdots, a_n$ 給出不同的結果，故它們在 $\mathfrak{S}^*$ 里都不相同．設 $N(n)$ 表 n 元合成的个数，根据定义得递推公式

$$(3) \qquad N(n) = N(n-1)N(1) + N(n-2)N(2) + \cdots + N(1)N(n-1).$$

又 $N(1) = 1$．对于任一个集合里的任一个二元合成，$N(n)$ 显然是所能导出不同 n 元合成的个数的上界．

要解递推公式 (3) 以得 $N(n)$ 的明确公式是不难的．我們可引入由冪級数

$$y = N(1)x + N(2)x^2 + \cdots + N(n)x^n + \cdots$$

来定义的"生成函数"．因 $N(1) = 1$，而

$$\begin{aligned} y^2 &= N(1)N(1)x^2 + [N(2)N(1) + N(1)N(2)]x^3 + \cdots \\ &= N(2)x^2 + N(3)x^3 + \cdots, \end{aligned}$$

故

$$y^2 - y + x = 0.$$

而

$$y = \frac{1-(1-4x)^{\frac{1}{2}}}{2} = \sum_{1}^{\infty} \frac{1\cdot 3\cdots(2n-3)}{1\cdot 2\cdots n} 2^{n-1}x^n,$$

所以

(4) $$N(n) = \frac{1\cdot 3\cdots(2n-3)}{1\cdot 2\cdots n} 2^{n-1}.$$ [1]

习 题 6

1. 在整数的集合 I 里定义二元合成 $f(x, y) = x + y^2$，求作所有导出的四元合成.

2. 对于一个給定的二元合成，我們可用归納方式定义 n 个 a 的簡单积为 a_1u 或 va_n，这里 u 为 $a_2, \cdots, a_n$ 的簡单积，v 为 $a_1, \cdots, a_{n-1}$ 的簡单积．証明：$\geqslant 2^r$ 个元素的任一个积可看作 r 个元素（它們自身也是积）的簡单积．

3. 广义結合律，冪 設給定的二元合成是可結合的，今将証 $a_1, a_2, \cdots, a_n$ 按这样次序作出所有可能的积必都相等．我們先用公式

$$\prod_1^1 a_i = a_1, \quad \prod_1^{r+1} a_i = \left(\prod_1^r a_i\right) a_{r+1}$$

来定义特殊积 $\prod_1^m a_i$，并証

引理 $$\prod_1^n a_i \prod_1^m a_{n+j} = \prod_1^{n+m} a_k.$$

証 $m = 1$ 时，由定义知这引理成立．今設 $m = r$ 时它是真的，則在 $m = r + 1$ 时，有

$$\prod_1^n a_i \prod_1^{r+1} a_{n+j} = \prod_1^n a_i \left(\left(\prod_1^r a_{n+j}\right) a_{n+r+1}\right)$$

$$= \left(\prod_1^n a_i \prod_1^r a_{n+j}\right) a_{n+r+1}$$

$$= \left(\prod_1^{n+r} a_k\right) a_{n+r+1}$$

---

1) 这公式可更簡单地写作 $N(n) = \dfrac{(2n-2)!}{n!(n-1)!}$．——著者注．

$$= \prod_{1}^{n+r+1} a_k,$$

所以也是眞的. 今考慮与$(a_1, a_2, \cdots, a_n)$連带的任一个积;由定义知，它是积uv，这里u是与$(a_1, a_2, \cdots, a_m)$連带的积，$1 < m < n$，而v是与$(a_{m+1}, \cdots, a_n)$連带的积. 由归納法,我們可假定$u = \prod_{i=1}^{m} a_i$及$v = \prod_{j=1}^{n-m} a_{m+j}$，故$uv = \prod_{k=1}^{n} a_k$. 于是，由$(a_1, a_2, \cdots, a_n)$决定的所有积都相等. 故此后这个唯一决定的积只須記作$a_1a_2 \cdots a_n$，可略去所有括号.

設所有$a_i = a$，則$a_1a_2 \cdots a_n$記作a^n，这元素叫做a的n冪. 由上面的說明可見，

(5) $$a^na^m = a^{n+m}, \quad (a^n)^m = a^{nm}.$$

如果$\mathfrak{S}$里的合成采用記号$+$，則須以

$$a_1 + a_2 + \cdots + a_n \text{ 代替 } a_1a_2\cdots a_n,$$
$$na \text{ 代替 } a^n.$$

关于冪的法則(5)这时变为关于倍数na的法則:

(5′) $$na + ma = (n + m)a, \quad m(na) = (mn)a.$$

4. 交換性 設a与b是半羣的元素，則可能有$ab \neq ba$. 例如，由§1里給出的半羣乘法表中，$\alpha\beta = \beta$，但$\beta\alpha = \gamma$. 設$\mathfrak{S}$里的元素a与b适合$ab = ba$，則說这两个元素可交換. 如果$\mathfrak{S}$里任意两个元素都是可交換时，則$\mathfrak{S}$叫做交換集合. 由归納法立見：如果$a_ib = ba_i$，$i = 1, 2, \cdots, n$，則

$$a_1 \cdots a_nb = ba_1 \cdots a_n.$$

次設元素$a_1, a_2, \cdots, a_n$都是可交換的，亦即对于所有i, j，$a_ia_j = a_ja_i$. 試考慮任一个积$a_{1'}a_{2'} \cdots a_{n'}$，这里$1', 2', \cdots, n'$是$1, 2, \cdots, n$的一种排列. 假定$a_n$出現于这积里的第$h$位，即$a_{h'} = a_n$，則有

$$a_{1'}a_{2'}\cdots a_{h'}\cdots a_{n'} = a_{1'}\cdots a_{(h-1)'}a_{(h+1)'}\cdots a_{(n-1)'}a_n.$$

使用归納法，我們可假定

$$a_{1'}\cdots a_{(h-1)'}a_{(h+1)'}\cdots a_{(n-1)'} = a_1a_2\cdots a_{n-1}.$$

故 $a_{1'}a_{2'}\cdots a_{n'}=a_1a_2\cdots a_n$.

由于(5)为真，故同一个元素的各幂都可交换. 又从討論中显見，如果 $ab=ba$，則

(6) $$(ab)^n=a^nb^n.$$

如采用加法記号，这結果化为

(6′) $$n(a+b)=na+nb.$$

5. 恒等元素及逆元素 設半羣 $\mathfrak{S}$ 有元素 e 对于 $\mathfrak{S}$ 里各元素 a 有 $ea=a$，則 e 叫做左恒等元素. 仿此，設 $\mathfrak{S}$ 有元素 f，对于各个 a 有 $af=a$，則 f 叫做右恒等元素.

例. (1) 正整数对于乘法所成的半羣有双側(=左及右)恒等元素 1. (2) 正整数对于加法所成的半羣无恒等元素. (3) 命 $\mathfrak{S}$ 为任一个集合，于 $\mathfrak{S}$ 里定义 $ab=b$，則 $\mathfrak{S}$ 是半羣，它的任一个元素都是左恒等元素；但若 $\mathfrak{S}$ 的元素不只一个，則这个集合无右恒等元素.

末了一例指出，半羣可有多个左(右)恒等元素，而无右(左)恒等元素. 但若 $\mathfrak{S}$ 同时含有一个左恒等元素 e 及一个右恒等元素 f，則必須 $e=f$. 这因为，e 是左恒等元素，$ef=f$；又因 f 是右恒等元素，$ef=e$. 由此可見，如果半羣有一个左恒等元素及一个右恒等元素，則每种不能多于一个. 特别是，如果有一个双側恒等元素存在，則它是唯一的[1].

此后双側恒等元素只叫做恒等元素，按惯例記做 1. 設 a 为 $\mathfrak{S}$ 的元素，如果 $\mathfrak{S}$ 里存在有一个元素 a'，使 $aa'=1$，則 a 叫做右正則元素，而 a' 叫做 a 的右逆元素. 仿此可定义左正則元素及左逆元素. 設 a 同时为左正則及右正則元素，則說它是单位(正則)元素. 此时存在有 a'，使 $aa'=1$，也存在有 a''，使 $a''a=1$. 因

$$a'=(a''a)a'=a''(aa')=a'',$$

故 $a'=a''$，这元素叫做 a 的逆元素；上面論証指明，它是唯一的[2]，我們記作 a^{-1}. 因 $aa^{-1}=1=a^{-1}a$，可見 a^{-1} 是正則元素，而 a 是

1) 設 e, e' 都是双側恒等元素，則因 e' 是双側恒等元素，故 $ee'=e$；又因 e 也是双側恒等元素，故 $ee'=e'$. 所以 $e=e'$——譯者注.

2) 設 a', a'' 都是 a 的逆元素，則 $aa'=1$，$a''a=1$. 于是 $a'=1a'=(a''a)a'=a''(aa')=a''\cdot 1=a''$. 故逆元素是唯一的——譯者注.

它的逆元素. 故有法則:

$$(a^{-1})^{-1} = a.$$

設 a 与 b 都是单位元素, 則 ab 也是单位元素; 这因为,

$$(ab)(b^{-1}a^{-1}) = 1 = (b^{-1}a^{-1})(ab).$$

故知 $(ab)^{-1} = b^{-1}a^{-1}$.

設以 + 表 $\mathfrak{S}$ 里运算, 則恆等元素記作 0. 如果 a 的逆元素存在, 則記作 $-a$. 故有

$$-(-a) = a \text{ 及 } -(a+b) = -b + (-a).$$

此后我們还把 $a + (-b)$ 写作 $a - b$.

6. 羣的定义及例

定义 2. 羣是半羣的一种, 它含有一个恆等元素, 且各元素都是单位元素.

所以羣是由集合 $\mathfrak{G}$ 及 $\mathfrak{G}$ 里二元合成所組成的一个代数系, 它适合下列各条件:

1. $(ab)c = a(bc)$.

2. $\mathfrak{G}$ 里存在有一个元素 1, 使 $a1 = a = 1a$.

3. 对于 $\mathfrak{G}$ 里每个 a, 在 $\mathfrak{G}$ 里存在有一个元素 a^{-1}, 使 $aa^{-1} = 1 = a^{-1}a$.

关于羣的集合部分, 也仿半羣中的办法, 叫做"羣 $\mathfrak{G}$". 下面是讀者熟悉的一些羣的例子.

例. (1) 实数的全体 R_+, 合成用加法. 此时, 数 0 是恆等元素, 而 a 的逆元素就是通常的 $-a$. (2) 复数的集合 C_+, 合成用加法. (3) 非零的实数的集合 R^*, 合成用乘法. 此时, 实数 1 是恆等元素, 而 a 的逆元素就是通常的倒数 a^{-1}. (4) 正实数的集合 Q, 合成用普通乘法. (5) 非零的复数的集合 C^*, 合成用乘法. (6) 絕对値为 1 的复数 $e^{i\theta}$ 的集合 U, 合成用乘法. (7) 1 的 n 个复 n 次根的集合 U_n, 合成用乘法. (8) 平面上繞一点 O 的旋轉的全体, 合成用积. 設取 O 为原点, 則經过角 θ 的旋轉可作为映照 $(x, y) \to (x', y')$, 用分析表出如

$$x' = x\cos\theta - y\sin\theta, \quad y' = x\sin\theta + y\cos\theta.$$

設 $\theta = 0$, 則得恆等变换, 它在旋轉的集合里起恆等元素的作用. 經过角 θ 的旋轉的逆旋轉是經过角 $-\theta$ 的旋轉. (9) 空間里繞一点 O 的旋轉的全体, 合成用积. (10) 平面上向量的集合, 合成用向量加法. 一个向量可用分析表为实数的二維組 (a, b), 它們分別为向量的 x-坐标与 y-坐标. 設 $v = (a, b)$, 而 $v' = (a', b')$, 則通常向量加法給出 $v + v' = (a + a', b + b')$. 零向量 $0 = (0, 0)$ 起恆等元素的作用, 而 v 的逆元素为 $-v = (-a, -b)$.

习 題 7

1. 命 $\mathfrak{G}$ 为实数二維組 (a, b) 的全体，其中 $a \neq 0$，如果 $\mathfrak{G}$ 里的合成由公式

$$(a, b)(c, d) = (ac, bc + d)$$

来定义，驗明：$\mathfrak{G}$ 是一个羣.

由半羣的討論，显見恆等元素在 $\mathfrak{G}$ 里是唯一的，而且 a 的逆元素也是唯一决定的. 設 a 与 b 是羣 $\mathfrak{G}$ 的任意两个元素，則綫性方程 $ax = b$ 在 $\mathfrak{G}$ 里有解为 $a^{-1}b$，而且是它仅有的解. 这因为，从 $ax = ax'$ 即有 $a^{-1}(ax) = a^{-1}(ax')$；因而 $x = x'$. 由此可見左相消律是成立的. 同理，方程 $ya = b$ 在 $\mathfrak{G}$ 里也有唯一的解，且右相消律成立. $ax = b$ 与 $ya = b$ 在 $\mathfrak{G}$ 里的可解性是羣的一个特性（参看下面习題的第 3 題）.

习 題 8

1. 設半羣的元素 e 适合 $e^2 = e$，这元素叫做同势元素[1]. 証明：羣里的同势元素是 $e = 1$.

2. 求証半羣如果具有下列各性质，則成为羣：

(a) $\mathfrak{G}$ 有一个右恆等元素 1_r；

(b) $\mathfrak{G}$ 的每个元素 a 对于 1_r 有一个右逆元素[2].

3. 設 $\mathfrak{G}$ 为半羣，且对于元素 a 与 b，方程 $ax = b$ 及 $ya = b$ 都是可解，証明：$\mathfrak{G}$ 是一个羣.

4. 如果相消律在一个有限半羣里成立，証明：这半羣是一个羣.

7. 子羣 令 $\mathfrak{S}'$ 是半羣 $\mathfrak{S}$ 的一个子集合，每当 a 与 b 都属于 $\mathfrak{S}'$ 时即有 $ab \in \mathfrak{S}'$，我們就說：$\mathfrak{S}'$ 是封閉的. 显然結合律在 $\mathfrak{S}'$ 里为眞. 故由 $\mathfrak{S}'$ 及导出的映照 $(a, b) \to ab$（a 与 b 属于 $\mathfrak{S}'$）所組成的代数系，$\mathfrak{S}', \cdot$ 成半羣，叫做半羣 $\mathfrak{S}$ 的子半羣. $\mathfrak{S}'$ 对于 $\mathfrak{S}$ 的合成可能成为羣，此时 $\mathfrak{S}'$ 叫做 $\mathfrak{S}$ 的子羣.

例. (1) 正整数的集合是(严格地說，决定)整数关于加法的羣 I_+ 里的一个子半羣. 偶整数的集合是 I_+ 的一个子羣. 更普遍地說，一个固定整数 m 的倍数 km 的全体是一个子羣. (2) 由数 1 与 -1 組成的集合是整数关于乘法的半羣里一个子羣.

今将証：設 $\mathfrak{S}$ 是带有恆等元素的任一个半羣，則 $\mathfrak{S}$ 的单位元

---

1) 同势元素也有譯作冪等元素——譯者注.

2) 設于 (b) 内，把"右"改为"左"，得来的代数系不一定成羣. 克里福得曾得它的結构，見数学紀录 (Annals of Math.)，卷 34，頁 865—871——作者注.

設取如$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$形二阶方陣的集合，易知右恆等元素为$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$，左逆元素为$\begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix}$. 但右逆元素不存在. 可見这集合不成为羣——譯者注.

素构成的子集合 $\mathfrak{G}$ 决定一个子羣. 命 a 与 b 为单位元素，前此已証得 $b^{-1}a^{-1}$ 是 ab 的逆元素，故 $ab\in\mathfrak{G}$. 因 $1\cdot1=1$，故 $1\in\mathfrak{G}$，且在 $\mathfrak{G}$ 里起恆等元素的作用. 最后，設 $a\in\mathfrak{G}$，因 $aa^{-1}=1=a^{-1}a$，故 $a^{-1}\in\mathfrak{G}$. 因此 $\mathfrak{G}$ 的每个元素在 $\mathfrak{G}$ 里各有逆元素. 我們把 $\mathfrak{G}$ 叫做 $\mathfrak{S}$ 的单位元素羣. 上面的例 (2) 就是:整数在乘法下的半羣里的单位元素羣. 将来可見，关于羣的許多重要的例都可从半羣的单位元素羣得出.

次从任意羣 $\mathfrak{G}$ 出发，决定它的子集合 $\mathfrak{H}$ 能成为 $\mathfrak{G}$ 的子羣的条件. 首先是，$\mathfrak{H}$ 必須封閉的. 其次，$\mathfrak{H}$ 須含有恆等元素 $1'$；但因 $(1')^2=1'$，显見(习题 8 的第 1 题) $1'$ 与 $\mathfrak{G}$ 的恆等元素 1 重合. 末了，設 $a\in\mathfrak{H}$，則 $\mathfrak{H}$ 里須存在一个元素 a' 使 $aa'=1=a'a$. 于是，a' 是 a 的一个逆元素；但因逆元素是唯一的，故 $a'=a^{-1}$. 綜上所述可見，要使羣 $\mathfrak{G}$ 的子集合 $\mathfrak{H}$ 成为 $\mathfrak{G}$ 的一个子羣，必須

1. $a, b\in\mathfrak{H}$ 时，則 $ab\in\mathfrak{H}$ (封閉性)；
2. $1\in\mathfrak{H}$；
3. $a\in\mathfrak{H}$，則 $a^{-1}\in\mathfrak{H}$.

这些条件也是子集合 $\mathfrak{H}$ 能使 $\mathfrak{H}, \cdot$ 成为 $\mathfrak{G}, \cdot$ 的一个子羣的充分条件. 这因为，从此可推得关于羣的公理 2 及 3；而結合性的条件在 $\mathfrak{G}$ 里本已成立，故在 $\mathfrak{H}$ 里必然成立是不待言的.

必須指出，羣 $\mathfrak{G}$ 自身可以看作是 $\mathfrak{G}$ 的一个子羣. 設 $\mathfrak{H}$ 是一个子羣，且是 $\mathfrak{G}$ 的眞子集合，則說: $\mathfrak{H}$ 是 $\mathfrak{G}$ 的眞子羣. 从定义或上述条件显見，仅由元素 1 构成的子集合也是 $\mathfrak{G}$ 的一个子羣，記它作 $\mathfrak{G}$ 的子羣 1 (用加法时，則記作 0).

习 题 9

1. 驗証:形狀如 $(1, b)$ 的二維組的子集合构成习題 7 的第一題里所述的羣的一个子羣.

2. 求証:羣 $\mathfrak{G}$ 的一个子集合 $\mathfrak{H}$ 成为一个子羣的充要条件是: a 与 b 属于 $\mathfrak{H}$ 时，$ab^{-1}\in\mathfrak{H}$.

3. 求証:羣的任一个有限子半羣必为一个子羣(参看习題 8 的第 4 題).

4. 設以 A 表 $\mathfrak{G}$ 的各子羣 $\mathfrak{H}$ 的任一个集合，求証:交 $\bigcap_A\mathfrak{H}$ 是一个子羣.

5. 設 a 是羣$\mathfrak{G}$的任一个元素，求証: 与 a 可交換的元素的集合 $\mathfrak{C}(a)$ 是 $\mathfrak{G}$ 的一个子羣.

8. 同构 我們先来考究这个基本概念的一个熟悉例子. 命 R_+ 是实数关于加法的羣, Q 是正实数关于乘法的羣. 就 R_+ 到 Q 內的映照 $x \to e^x$ 来看, 它是 R_+ 到 Q 上的 1—1 映照. 逆映照是 $z \to \log z$. 还有基本性質

$$e^{x+y} = e^x e^y.$$

故設 (a) 先在 R_+ 里作两数的羣合成, 然后求在 Q 里的象, 或 (b) 先求在 Q 里的象, 然后对于这些象作羣合成, 都得出同样結果. 因为我們不考虑羣里各元素的实質, 而只对它們的合成感到兴趣, 而这两个例子里的合成刚好有相同性質; 故从抽象观点来說, 羣 R_+ 与 Q 在性質上无所区别. R_+ 与 Q 間的密切关系可依下面的定义說成这两个羣是同构的.

定义 3. 設在两个羣 $\mathfrak{G}$ 与 $\mathfrak{G}'$ 間存在有 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 上的 1—1 映照 $x \to x'$, 使 $(xy)' = x'y'$, 則說: $\mathfrak{G}$ 与 $\mathfrak{G}'$ 是同构的.

适合定义里条件的映照叫做 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 上的同构. 設 $\mathfrak{G}$ 与 $\mathfrak{G}'$ 是同构的, 两者間可有很多的同构存在. 例如, 設 a 是 $\neq 1$ 的任一个正整数, 則映照 $x \to a^x$ 是 R_+ 到 Q 上的一个同构. 同构的羣常被說是抽象等价的. 設 $\mathfrak{G}$ 与 $\mathfrak{G}'$ 是同构的, 就記作 $\mathfrak{G} \cong \mathfrak{G}'$. 显然, 两羣間的同构是一种等价关系. 这因为, 恆等映照是 $\mathfrak{G}$ 到自身上的一个同构. 如果 $a \to a'$ 是 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 上的一个同构, 則逆映照 $a' \to a$ 是 $\mathfrak{G}'$ 到 $\mathfrak{G}$ 上的一个同构. 最后, 設 $a \to a'$ 是 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 上的一个同构, 而 $a' \to a''$ 是 $\mathfrak{G}'$ 到 $\mathfrak{G}''$ 上的一个同构, 則 $a \to a''$ 是 $\mathfrak{G}$ 到 $\mathfrak{G}''$ 上的一个同构.

习　题　10

1. 設 $x \to x'$ 是一个同构, 求証: 1 的象 $1'$ 是第二个羣的恆等元素, 并証: $(a^{-1})' = (a')^{-1}$.

2. 映照 $\theta \to e^{i\theta}$ 是否为 R_+ 到由絕对值为 1 的复数組成的乘法羣上的一个同构呢?

9. 变換羣 設 S 是一个任意集合, 而 $\mathfrak{T}(S)$ 是 S 到自身內的变換所成的半羣, 則 $\mathfrak{T}$ 有恆等变換, 即恆等映照 $x \to x$. 今考究 $\mathfrak{T}(S)$ 的单位元素的子羣 $\mathfrak{G}(S)$. 我們知道: 如果 α 是 S 到 S 上的 1—1 映照, 則逆映照 α^{-1} 具有性質 $\alpha\alpha^{-1} = 1 = \alpha^{-1}\alpha$. 反之, 設 α 是 $\mathfrak{T}(S)$

里任一个元素，而有逆元素β存在，使 $\alpha\beta = 1 = \beta\alpha$，則任一个 $x = (x\beta)\alpha \in S\alpha$，故 α 把 S 映照到它自身上．不仅如此，如果 $x\alpha = y\alpha$，則 $(x\alpha)\beta = (y\alpha)\beta$，而 $x = y$．于是，α 是 1—1 映照．这証明：$\mathfrak{G}(S)$ 恰是 S 到自身上的 1—1 映照的集合，叫做集合 S 的 1—1 变换（或置换）的羣．

更普遍的情况是羣 $\mathfrak{G}(S)$ 的任一个子羣，我們叫它做（S 里）一个变换羣．如果回忆一个子集合 $\mathfrak{H}$ 能成子羣的条件，就可知集合 S 到自身上的 1—1 变换的集合 $\mathfrak{H}$ 如果适合下列各条件，則决定一个变换羣：

1. 設 $\alpha, \beta \in \mathfrak{H}$，則积 $\alpha\beta \in \mathfrak{H}$．
2. 恆等映照 $x \rightarrow x$ 属于 $\mathfrak{H}$．
3. 設 $\alpha \in \mathfrak{H}$，則逆映照 α^{-1} 属于 $\mathfrak{H}$．

今考究 S 是 n 个数 $1, 2, \cdots, n$ 的集合这一特款．S 的置换的羣 $\mathfrak{G}(S)$ 叫做 n 次对称羣，記作 S_n．它的元素 α 用形如

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ 1\alpha & 2\alpha & \cdots & n\alpha \end{pmatrix}$$

的記号表出，并且可用这样的表示来計算羣 S_n 的阶（S_n 里元素的个数）．元素 1α 显然是任意的，故选择作第一位的数可有 n 种方法．因为記号的第二行上数字不許重复，故选择作第二位的数有 $n-1$ 种方法，第三位的数有 $n-2$ 种方法等等．所以总共得 $n!$ 个記号，从而 S_n 共有 $n!$ 个元素．

习　　題 11

1. 設

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix},$$

計算 $\alpha\beta$, $\beta\alpha$, 及 α^{-1}．

2. 写出 S_3 的元素，并作出这个羣的乘法表．

3. 驗証下列变换成一个变换羣：

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

4. §6 里那些个例子是变换羣？

5. 驗証由法則 $x \rightarrow ax + b$, $a \neq 0$ 給出直綫的变换的集合成一个变换羣．証明这个羣与习題 7 的第 1 題里給出的羣是同构的．

6. 驗証由 $(x, y) \to (x + a, 0)$ 所定义的平面上变換的全体关于积合成組成一个羣. 它是一个变换羣嗎?

10. 羣用变換羣实現 从历史上說，羣論最初只处理变換羣. 后来为着要使变換羣上那些仅限于积合成而不牵連到施行变換的集合 S 的性質能够以最簡单与最直接的方式引出，才导入抽象羣的概念. 我們很自然地要問:抽象概念与实际是否完全符合,亦即它所包括的这类代数系是否刚好与这类变換羣一致? 这問題从下面凱萊 (Cayley) 的基本定理得到肯定的答复.

定理 1. 任一个羣必同構于一个变換羣.

証 我們将要定义的变換羣是作用于給定羣的集合 $\mathfrak{G}$ 里. 把羣 $\mathfrak{G}$ 的每个元素 a 与集合 $\mathfrak{G}$ 到自身內的映照 $x \to xa$ 联系起来. 这映照記作 a_r, 叫做由 a 决定的右乘变換. 因为右相消律成立,故 a_r 是 1—1 映照. 因任一个元素 b 可写成 $(ba^{-1})a = (ba^{-1})a_r$, 故 a_r 是 $\mathfrak{G}$ 到自身上的映照. 于是, a_r 属于集合 $\mathfrak{G}$ 的 1—1 变換的羣. 今要証 $\mathfrak{G}_r = \{a_r\}$ 的全体是 $\mathfrak{G}$ 里一个变換羣. 首先考究积 a_rb_r. 它把 x 变为 $(xa)b$. 由結合律, $(xa)b = x(ab)$, 故 a_rb_r 与 $(ab)_r$ 有同样作用. 于是,

$$a_rb_r = (ab)_r \tag{7}$$

属于 $\mathfrak{G}_r$. 其次,我們知, $1 = 1_r$ 属于 $\mathfrak{G}_r$. 最后,由 (7) 得 $a_r(a^{-1})_r = 1_r = (a^{-1})_ra_r$, 故 $a_r^{-1} = (a^{-1})_r$ 属于 $\mathfrak{G}_r$. 因此 $\mathfrak{G}_r$ 是一个变換羣. 今考究羣 $\mathfrak{G}$ 到羣 $\mathfrak{G}_r$ 上的对应 $a \to a_r$. 如果 $a \neq b$, 则 $1a_r = a \neq b = 1b_r$, 从而 $a_r \neq b_r$; 故 $a \to a_r$ 是 1—1 映照. 因 (7) 成立, 故映照 $a \to a_r$ 是一个同构,而証明完成.

我們称同构 $a \to a_r$ 是 $\mathfrak{G}$ 用变換羣(右)正則实現. 应該指出, 如果 $\mathfrak{G}$ 是 n 阶有限羣,则 $\mathfrak{G}_r$ 是对称羣 S_n 的一个子羣. 故得

系. 任一个 n 階有限羣与 S_n 的一个子羣是同構的.

例. (1) R_+ 是实数的加法羣. 如果 $a \in R_+$, 則 a_r 为平移变换 $x \to x' = x + a$. (2) R^* 是非零实数的乘法羣. a_r 是伸縮变換 $x \to x' = ax$. (3) 实数二維組 (a, b) 的羣, $a \neq 0$, 合成法則是

$$(a, b)(c, d) = (ac, bc + d),$$

这里 $(c, d)_r$ 把 (x, y) 映照到 (x', y'),

$$x' = cx, \quad y' = cy + d.$$

$\mathfrak{G}$ 用变换羣实現的另一种是使用左乘变换. $\mathfrak{G}$ 到自身內的映照 $x \to ax$ 叫做左乘变换, 記作 a_l. 与右乘变换相似, 我們易知: a_l 是 $\mathfrak{G}$ 到自身上的 1—1 映照, 而且 a_l 的集合 $\mathfrak{G}_l$ 是一个变换羣. 后者的証明中,除

(8) $$a_l b_l = (ba)_l$$

这一改变外,完全与对于 $\mathfrak{G}_r$ 的証明相同. 这里 (8) 是由

$$x a_l b_l = b(ax) = (ba)x = x(ba)_l$$

得出. 映照 $a \to a_l$ 是 $\mathfrak{G}$ 到 $\mathfrak{G}_l$ 上的 1—1 映照; 一般說来, 它不是一个同构. 要得同构須以映照 $a \to a_l^{-1} = (a^{-1})_l$ 代替它. 这因为,

$$(ab)_l^{-1} = (b_l a_l)^{-1} = a_l^{-1} b_l^{-1}.$$

我們把同构 $a \to a_l^{-1}$ 叫做 $\mathfrak{G}$ 的左正則实現.

因 $x a_l b_r = (ax)b$, $x b_r a_l = a(xb)$, 故由 $\mathfrak{G}$ 里結合律得 $a_l b_r = b_r a_l$; 它对于 $\mathfrak{G}$ 里所有 a, b 都成立. 故属于集合 $\mathfrak{G}_r$ 的任一个变换与属于 $\mathfrak{G}_l$ 的任一个变换可以交换. 逆定理也是成立的, 即: 如果 β 是 $\mathfrak{G}$ 里任一个变换, 与所有 $a_l(a_r)$ 可交换, 則 β 是一个右(左)乘变换. 这因为,如果 $b = 1\beta$, 則有

$$x\beta = (x1)\beta = (1x_l)\beta = (1\beta)x_l = x(1\beta) = xb.$$

故 $\beta = b_r$.

习　题　12

1. 写出 S_3 的正則实現.

11. 循环羣,元素的阶 設 M 是羣 $\mathfrak{G}$ 的任一个非空子集合, 命 $\{\mathfrak{H}\}$ 是 $\mathfrak{G}$ 里含有集合 M 的各子羣的集合. 因集合 $\{\mathfrak{H}\}$ 含有 $\mathfrak{G}$, 故为非空集合. 它的交 $\cap\mathfrak{H}$ 是 $\mathfrak{G}$ 的子羣 (习題 9 的第 4 題), 記作 $[M]$, 叫做由集合 M 生成的 $\mathfrak{G}$ 的子羣. 集合 $[M]$ 具有下列各性質: (1) $[M]$ 是 $\mathfrak{G}$ 的一个子羣. (2) $[M] \supseteq M$. (3) 如果 $\mathfrak{H}$ 是 $\mathfrak{G}$ 的任一个子羣, 它包含 M 为子集合, 則 $\mathfrak{H} \supseteq [M]$. 这些性質显然也是 $[M]$ 的特性. 这因为,如果 $\mathfrak{K}$ 是 $\mathfrak{G}$ 的一个子集合, 能适合(关于 M 的) (1), (2) 及 (3), 則因 $\mathfrak{K}$ 是包含 M 的一个子羣,故有 $\mathfrak{K} \supseteq [M]$. 由对称性得 $[M] \supseteq \mathfrak{K}$. 故 $\mathfrak{K} = [M]$.

利用这特点,可以明确求得 $[M]$ 的元素. 我們肯定这些元素

恰是各个有限积 $a_1 a_2 \cdots a_n$（n 为任意的），这里 $a_i \in M$，或 a_i 是 M 里元素的逆元素．令 $\mathfrak{K}$ 为这些积的集合，易知 $\mathfrak{K}$ 是 $\mathfrak{G}$ 的一个子羣，它含有 M．另一方面，設 $\mathfrak{H}$ 是 $\mathfrak{G}$ 的一个子羣，也含有 M，则 $\mathfrak{H}$ 含有每个 $a \in M$，且当每个 $a \in M$ 时，$\mathfrak{H}$ 都含有 a^{-1}．故 $\mathfrak{H}$ 含有 $\mathfrak{K}$．因此 $\mathfrak{K}$ 适合 (1)，(2) 及 (3)；从而 $\mathfrak{K} = [M]$．

今来考究 $M = \{a\}$ 这一特款，它是由一个元素 a 組成的集合；我們把 $[M]$ 写作 $[a]$，并把这个子羣叫做由 a 生成的(循环)羣．設在羣 $\mathfrak{Z}$ 里有元素 a 存在，使 $\mathfrak{Z} = [a]$，则 $\mathfrak{Z}$ 叫做循环羣．元素 a 叫做 $\mathfrak{Z}$ 的生成元素．上面的說明指出，$[a]$ 是由元素 a^n $(n > 0)$，1，及 $(a^{-1})^n$ $(n > 0)$等組成．現在定义 $a^0 = 1$ 及 $a^{-n} = (a^{-1})^n$ $(n > 0)$，则 $[a]$ 即由 a 的整数幂組成．

由各种情形的考究，可使指数的基本定律 (5) 拓广到所有整数幂．例如，設 $n > |m|$，而 $m < 0$，则

$$a^n a^m = a^n a^{-|m|} = a^n (a^{-1})^{|m|} = a^{n-|m|} = a^{n+m}.$$

至于其余情形託讀者自己去驗証．我們可由指数定律或直接地看出，$[a]$ 是一个交換羣．下面是一些关于循环羣的熟知例子．

例．(1) 設 I_+ 是整数的加法羣．由归納法公理显見，含有 1 的正整数的集合，如果对于加法封閉，则它含有一切正整数．由此可見，$I_+ = [1]$．显然还有 $I_+ = [-1]$；而且如果 $k \neq 1, -1$，则 $1 \notin [k]$．故 1 与 -1 是 I 的唯一生成元素．

(2) 令 U_n 是由1的复 n 次根組成的羣，则 U_n 由复数 $e^{\frac{2k\pi}{n}i}$，$k = 0, 1, \cdots, n-1$，构成．使用复数的标准几何表示，即知这些数是由正 n 角形的頂点表出，而这个正 n 角形是內接于单位圓，且有 $(1, 0)$ 为一个頂点．設令 $e^{\frac{2\pi i}{n}} = \rho$，则 U_n 的元素是 $1, \rho, \rho^2, \cdots, \rho^{n-1}$．故 U_n 是 n 阶循环羣．

令 $\mathfrak{Z}$ 是一个循环羣，a 是它的生成元素．考究 I_+ 到 $\mathfrak{Z}$ 上的映照 $n \to a^n$．这对应具有性質

$$m + n \to a^{m+n} = a^m a^n.$$

所以，如果这映照是 1—1 的，则它是 I_+ 到 $\mathfrak{Z}$ 上的同构．

次設这映照不是 1—1 的，则有 $m \neq n$ 而使 $a^m = a^n$．我們可假定 $n > m$．于是，

$$a^{n-m} = a^n a^{-m} = a^m a^{-m} = 1.$$

故有正整数 p 存在，使 $a^p = 1$．令 r 是具有这个性質的最小正整

数，则元素 $1, a, \cdots, a^{r-1}$ 肯定是不同的，并且 $\mathfrak{Z}$ 的每个元素属于这集合內. 这因为，如果 k, l 各取 $0, 1, \cdots, r-1$ 里的数，$k \neq l$，而有 $a^k = a^l$ 时，则必有 p 存在，$0 < p < r$，且 $a^p = 1$. 这与 r 的挑选方法矛盾. 次令 a^n 是 $\mathfrak{Z}$ 的任一个元素，令 $n = qr + s$，$0 \leqslant s < r$，则

$$a^n = a^{qr+s} = a^{qr}a^s = (a^r)^q a^s = a^s.$$

这証实了我們的說法是对的. 故 $\mathfrak{Z}$ 是一个 r 阶有限羣.

由此可知，如果 $\mathfrak{Z}$ 是无限羣，则映照 $n \to a^n$ 必为 1—1 的. 故任一个无限循环羣同构于 I_+. 于是，任意两个无限循环羣都成同构. 其次，我們要証：任意两个同阶的有限循环羣是同构的. 令 $\mathfrak{Z} = [a]$，及 $\mathfrak{W} = [b]$ 都是 r 阶，则 $[a]$（或 $[b]$）的阶 r 是能使 $a^r = 1$（$b^r = 1$）的最小正整数. 令 h 是能使 $a^h = 1$ 的任一个整数. 命 $h = rq + s$，$0 \leqslant s < r$，则由 $a^h = 1$ 得

$$a^s = a^s 1^q = a^s (a^r)^q = a^{s+rq} = a^h = 1.$$

故由 r 的极小性知 $s = 0$. 于是，$r \mid h$. 今設 $a^n = a^m$，则 $a^{n-m} = 1$. 故 $n - m = rq$. 于是，$1 = b^{rq} = b^{n-m}$，而 $b^n = b^m$. 作映照 $a^n \to b^n$，则可断言这对应是单值的. 根据对称性，由 $b^n = b^m$ 可推出 $a^n = a^m$. 所以，这个映照是 1—1 的. 显然，

$$a^n a^m = a^{n+m} \to b^{n+m} = b^n b^m.$$

故 $a^n \to b^n$ 是一个同构. 这証明了下面的

定理 2. 同階的任意两个循环羣都是同構的.

循环羣的概念使我們对于任意羣 $\mathfrak{G}$ 的元素获得初步分类. 設 a 是 $\mathfrak{G}$ 的任一个元素，则按照 $[a]$ 是无限羣或是 r 阶有限羣，而說 a 是**无限阶**或是**有限 r 阶**的元素. 在前一情形下，如果 n 是 $\neq 0$ 的任一个整数，则 $a^n \neq 1$；而在后一情形下，则有 $a^r = 1$，这里的 r 是能使 $a^r = 1$ 的最小正整数.

循环羣在各种羣中算是最簡单的. 因此，关于羣方面大多数問題在这类型上容易得出回答是不足为奇的. 例如，对于一个給定的羣，要去决定它的一切子羣，一般說来，这是一个很难的課題；但我們知道，这在循环羣可以很簡单地解决的.

令 $\mathfrak{B}$ 是循环羣 $\mathfrak{Z}=[a]$ 的一个子羣. 先設 $\mathfrak{B}\neq 1$, 則有正整数 m 存在使 $a^m\in\mathfrak{B}$. 这因为, 有整数 $m\neq 0$ 存在, 使 $a^m\in\mathfrak{B}$; 并且如果 $a^m\in\mathfrak{B}$, 則 $(a^m)^{-1}=a^{-m}$ 也属于 $\mathfrak{B}$. 今設 s 为最小正整数使 $a^s\in\mathfrak{B}$. 我們要証: $\mathfrak{B}=[a^s]$, 而且对应 $\mathfrak{B}\to s$ 是 1—1 映照. 要証这些結果, 令 $c=a^m$ 是 $\mathfrak{B}$ 里任一个元素. 命 $m=sq+u$,这里 $0\leqslant u<s$, 則 $a^u=a^m(a^s)^{-q}\in\mathfrak{B}$. 故由 s 的极小性得 $u=0$. 于是, $c=a^m=(a^s)^q$, 而 $\mathfrak{B}=[a^s]$. 又因为,如果 $\mathfrak{B}\to s$ 及 $\mathfrak{B}'\to s$, 則 $\mathfrak{B}=[a^s]=\mathfrak{B}'$, 显然这映照是 1—1 的.

設 $\mathfrak{Z}$ 为无限循环羣, 則映照 $\mathfrak{B}\to s$ 是在正整数集合上的一个映照. 这因为,如果取任一个正整数 s, 因为能使 $a^p\in[a^s]$ 的最小正整数 p 是 s 自身,故 $[a^s]\to s$.

次設 $\mathfrak{Z}$ 是 r 阶有限羣, 我們要証:映照 $\mathfrak{B}\to s$ 是在 $<r$ 而为 r 的因子的正整数集合上的映照. 因为 $1=a^r\in\mathfrak{B}$, 前此用过的論証指出, r 是 s 的倍数,即 $s|r$. 另一方面,令 s 为 r 的任一个因子,并令 $r=st$, 則 $(a^s)^t=1$; 但若 $0<t'<t$, 則 $(a^s)^{t'}\neq 1$. 故 t 是 $[a^s]$ 的阶. 今設 s' 是最小正整数使 $a^{s'}\in[a^s]$, 則因 $[a^{s'}]=[a^s]$ 也使 $r=s't$, 故 $s=s'$. 于是, $[a^s]\to s$.

这就証明了下面的

定理 3. 令 $\mathfrak{Z}$ 是循环羣, 以 a 为生成元素, 並令 $\mathfrak{B}$ 是 $\mathfrak{Z}$ 的任一个子羣,但 $\neq 1$. 如果 s 是最小正整数使 $a^s\in\mathfrak{B}$, 則 $\mathfrak{B}=[a^s]$. 設 $\mathfrak{Z}$ 是无限羣,則对应 $\mathfrak{B}\to s$ 是 $\neq 1$ 的子羣的集合到正整數集合上的一个 1—1 映照. 設 $\mathfrak{Z}$ 是 r 階有限羣, 則这映照是 $\neq 1$ 的子羣的集合到小于 r 而为 r 的正因子的集合上的 1—1 映照.

設 $\mathfrak{Z}$ 是无限羣, 則这个对应可由映照 $1\to 0$ 扩张到包括仅由 1 組成的子羣 1. 在有限羣情形則作映照 $1\to r$. 故在所有情形都得 $\mathfrak{B}=[a^s]$. 我們还知道, 在有限羣情形下, 如果 $\mathfrak{B}\to s$, 則 $\mathfrak{B}$ 的阶是 $r/s=t$. 故得出联系这子羣的阶与 $\mathfrak{B}$ 的另一个 1—1 对应. 这結果可述为

定理 4. 令 $\mathfrak{Z}$ 是 $r(<\infty)$ 階循环羣,則 $\mathfrak{Z}$ 的任一个子羣的階是 r 的一个因子;如果 t 是 r 的任一个正因子,則 $\mathfrak{Z}$ 拥有一个而且

只有一个 t 階子羣.

习慣上以 $d(r)$ 表整数 r 的正因子的个数，故知 $\mathfrak{Z}$ 含有 $d(r)$ 个子羣.

习　题　13

1. 把 12 阶循环羣的子羣列成一表.

2. 令 $\mathfrak{Z}=[a]$ 是 $r(<\infty)$ 阶循环羣，求証: a^m 的阶是 $[m,r]/m=r/(m,r)$.

3. 求証: r 阶循环羣恰含有 $\phi(r)$ 个生成元素，这里 $\phi(r)$ (欧拉 (Euler) 的 ϕ-函数)表 $<r$ 而与 r 互素(亦即 $(r,h)=1$) 的正整数 h 的个数.

4. 求証: 下列两性质的每个都是 r 阶循环羣 $\mathfrak{G}$ 的 $t(r=st)$ 阶子羣 $\mathfrak{H}$ 的特点:
   (1) $\mathfrak{H}$ 是 $\mathfrak{G}$ 的元素的 s 冪的集合;
   (2) $\mathfrak{H}$ 是能使 $h^t=1$ 的元素 h 的集合.

12. 置换的初等性质 使 $\{1,2,\cdots,n\}$ 內元素 $i_1,i_2,\cdots,i_r$ 的集合按方式

(9) $$i_1\gamma=i_2,\ i_2\gamma=i_3,\ \cdots,\ i_{r-1}\gamma=i_r,\ i_r\gamma=i_1$$

循环替换，并保持其余元素不变的置换 γ 叫做循环. 这种的 γ 記作 $(i_1 i_2\cdots i_r)$. 显然我們也可写做

$$\gamma=(i_2 i_3\cdots i_r i_1)=(i_3 i_4\cdots i_r i_1 i_2)=\cdot\ \cdot.$$

如果两个循环 γ 与 γ' 的記号中不含有公共文字，就說它們是不相交的. 在这情形下，数字会被这些变換中的一个所改变时，对于其余变換必不生改变. 所以，如果 i 是任一个数字，$i\gamma\neq i$，則 $i\gamma'\gamma=i\gamma$; 又因为 $i\gamma^2\neq i\gamma$，故 $i\gamma\gamma'=i\gamma$. 同理，設 $i\gamma'\neq i$，則 $i\gamma\gamma'=i\gamma'\gamma$. 又設 $i\gamma=i$ 及 $i\gamma'=i$，則 $i\gamma\gamma'=i\gamma'\gamma$. 故 $\gamma\gamma'=\gamma'\gamma$，亦即任意两个不相交循环必可交换.

任一个置换可写成不相交的循环的积. 例如，設

$$\alpha=\begin{pmatrix}1&2&3&4&5&6&7&8\\3&6&5&4&8&2&7&1\end{pmatrix},$$

則

$$1\alpha=3,\quad 3\alpha=5,\quad 5\alpha=8,\quad 8\alpha=1;$$
$$2\alpha=6,\quad 6\alpha=2,\quad 4\alpha=4,\quad 7\alpha=7;$$

由此得

$$\alpha=(1358)(26)(4)(7).$$

对于任一个 α，一般可从 1，2，$\cdots$，n 里任一个数字，譬如 i_1，开始，作 $i_1\alpha=i_2$, $i_2\alpha=i_3$, $\cdots$，直至遇到表中先前已出現的数字为止. 当 $i_{r+1}=i_r\alpha=i_1$ 时，就开始这样的重复出現；这因为 $i_k=i_1\alpha^{k-1}$，所以如果 $i_k=i_l$, $l>k$，則 $i_1\alpha^{k-1}=i_1\alpha^{l-1}$，而 $i_1\alpha^{l-k}=i_1$. 因此，α 把数字 i_1, i_2, $\cdots$, i_r 作循环置换. 如果 $r<n$，則可在这个集合以外找出一个 j_1. 如果 $j_1\alpha^n=i_1\alpha^q$，則 $j_1=i_1\alpha^{q-n}$ 就要属于上面的集合，这与假設矛盾了. 故又得一个新集合 $\{j_1, j_2, \cdots, j_s\}$，它也被 α 循环置换，并且与上面的集合无公共元素. 这样継續到集合 $\{1, 2, \cdots, n\}$ 里的数字用完为止. 比較在任一个数字上的作用，显見

(10) $\qquad \alpha=(i_1i_2\cdots i_r)(j_1j_2\cdots j_s)\cdots(l_1l_2\cdots l_u)$,

这些循环都是不相交的.

循环 (i) 是恆等映照. 这种循环可从 (10) 中弃去；因此可假定 (10) 里的 $r, s, \cdots, u>1$. 由于这样得来的分解可导出

$$i_1\alpha=i_2, \cdots, \quad i_{r-1}\alpha=i_r, \quad i_r\alpha=i_1; \cdots;$$

$$l_1\alpha=l_2, \cdots, l_{u-1}\alpha=l_u, l_u\alpha=l_1,$$

而且所有其余数字都是不变的，故这分解是唯一的. 設分解 α 为不相交循环如 (10)，則我們可把 α 与整数

(11) $\qquad N(\alpha)=(r-1)+(s-1)+\cdots+(u-1)$

結合起来.

(ab) 形的循环叫做**对換**. 容易驗証

(12) $\qquad (i_1i_2\cdots i_r)=(i_1i_2)(i_1i_3)\cdots(i_1i_r)$.

故由 (10) 可見：α 是 $N(\alpha)$ 个对換的积. 今来証明：**設 $N(\alpha)$ 为偶(奇)数，則 α 化为对換的积的任一个分解中必含有偶(奇)数个因子.** 要証这定理，需用下列两公式：

$$(ac_1c_2\cdots c_hbd_1\cdots d_k)(ab)=(ac_1\cdots c_h)(bd_1\cdots d_k),$$

$$(ac_1\cdots c_h)(bd_1\cdots d_k)(ab)=(ac_1\cdots c_hbd_1\cdots d_k).$$

由此可見，如果 a 与 b 出現于 α 的同一循环里，則 $N(\alpha(ab))=N(\alpha)-1$；如果 a 与 b 出現于 α 的不同循环里，則 $N(\alpha(ab))=N(\alpha)+1$. 总之，

(13) $$N(\alpha(ab)) = N(\alpha) \pm 1.$$
今設 α 是 m 个对换的积，令 $\alpha = (ab)(cd)\cdots(pq)$. 因 $(ab)^{-1} = (ab)$，故知

$$\alpha(pq)\cdots(cd)(ab) = 1.$$

因 $N(1) = 0$，反复使用 (13)得

$$0 = N(\alpha)\ \overbrace{\pm 1 \pm 1 \pm \cdots \pm 1}^{m}.$$

故 $N(\alpha)$ 是 m 項 $+1$ 或 -1 的和. 因此，$N(\alpha)$ 为偶数必須而且只須 m 为偶数. 这就証明了上面的結果.

把 α 分解为对换的积时，我們根据它所含因子的个数为偶数或奇数而将 α 叫做**偶或奇置換**. 設 α 是 m 个对换的积，而 β 是 q 个对换的积，則 $\alpha\beta$ 是 $m+q$ 个对换的积，而 α^{-1} 是 m 个对换的积. 故設 α 与 β 都是偶置換，則 $\alpha\beta$ 也是偶置換；但若 α 是偶(奇)置換，而 β 是奇(偶)置換，則 $\alpha\beta$ 是奇置換；又若 α 与 β 都是奇置換，則 $\alpha\beta$ 是偶置換. 設 α 是偶置換，則 α^{-1} 也是偶置換. 这些法則还指出：偶置換的集合 A_n 是 S_n 的一个子羣，叫做**交代羣**.

习 題 14

1. 試将 S_4 的元素写成. (1) 不相交循环的积，(2) 对换的积. 决定 A_4 的元素.
2. 設 $n \geqslant 3$，求証：A_n 的任一个元素是**三元循环** (abc) 的积.

13. 羣的陪集分解 先設 $\mathfrak{G}$ 是作用于集合 S 的一个任意变換羣，則 $\mathfrak{G}$ 在 S 內用下面所述的法則来定义一个等价关系：設对于 $\mathfrak{G}$ 內某个 α，而有 $y = x\alpha$，則 $x \equiv y \pmod{\mathfrak{G}}$ (讀做：x 等价于 y，模 $\mathfrak{G}$). 由变換羣的定义立見，这关系具有反身、对称及传递性. 有时会遇到，S 的任意两个元素在这样意义下都成等价；此时，$\mathfrak{G}$ 被說是在 S 內成**传递羣**. 一般說来，我們可得出把 S 分解为非相交的等价类；这种等价类，我們叫做 S 关于 $\mathfrak{G}$ 的**传递集合**.

作为这类型分解的例子，命 $S = \{1, 2, \cdots, n\}$ 及 $\mathfrak{G} = [\alpha]$，这里 $\alpha \in S_n$. 設 $\alpha = (i_1 i_2 \cdots i_r)\cdots(l_1 l_2 \cdots l_u)$ 是 α 化为不相交循环的分解，显然 $\{i_1, i_2, \cdots, i_r\}, \cdots, \{l_1, l_2, \cdots, l_u\}$ 都是 $[\alpha]$ 的传递集合，其余的传递集合都只含有一个元素. 前节所考究的

数 $N(\alpha)$ 今定义为 $\sum(r-1)$，这里 r 表示任一个传递集合内元素的个数，而且就对于这些集合来求和. 这个説明又一次指出，$N(\alpha)$ 是唯一的，而且一般会使人或多或少地更能了解前节的討論.

今設 $\mathfrak{G}$ 为任一个羣,而 $\mathfrak{H}$ 是 $\mathfrak{G}$ 的一个子羣. 令 $\mathfrak{H}_r'$ 是 $\mathfrak{G}$ 里用 $\mathfrak{H}$ 的元素决定的右乘变换的集合;亦即 $\mathfrak{H}_r'$ 是映照 $x \to xh$ 的集合,这里 $x \in \mathfrak{G}$, h 是 $\mathfrak{H}$ 里固定元素. 因 $\mathfrak{H}$ 是 $\mathfrak{G}$ 的一个子羣, $\mathfrak{H}_r'$ 是 $\mathfrak{G}_r$ 的一个子羣,故 $\mathfrak{H}_r'$ 是作用于集合 $\mathfrak{G}$ 的一个变换羣. 今考究由 $\mathfrak{H}_r'$ 决定的传递集合. 为簡单計,以 $x \equiv y (\mathrm{mod}\ \mathfrak{H})$ 代替 $x \equiv y (\mathrm{mod}\ \mathfrak{H}_r')$. 由定义,这意味着 $\mathfrak{H}$ 里存在一个 h 使 $y=xh$,或等价于說 $x^{-1}y \in \mathfrak{H}$. 与 x 同余(等价)的元素的传递集合叫做 x 关于 $\mathfrak{H}$ 的**右陪集**.

今对于右陪集引入一个方便記法. 一般而論，設 A 与 B 是羣 $\mathfrak{G}$ 的子集合,我們以 AB 記积 ab 的集合,这里 $a \in A, b \in B$. 因此，$(AB)C$ 是积 $(ab)c$ 的集合，这里 $a \in A$, $b \in B$, $c \in C$. 因 $(ab)c = a(bc)$，故任一个这样的积都属于 $A(BC)$；于是，$(AB)C \subseteq A(BC)$. 同理可証 $A(BC) \subseteq (AB)C$，故 $(AB)C = A(BC)$. 如果由一个元素 x 构成的集合記作 x，显然 x 关于 $\mathfrak{H}$ 的右陪集是元素 xh 的集合，这里 $h \in \mathfrak{H}$. 故这个陪集即是 $x\mathfrak{H}$. 无疑地，$\mathfrak{G} = \bigcup x\mathfrak{H}$，而且对于任意 $x\mathfrak{H}$ 与 $y\mathfrak{H}$ 或 $x\mathfrak{H} = y\mathfrak{H}$，或 $x\mathfrak{H} \cap y\mathfrak{H} = \phi$.

例. (1) 命 I_+ 是整数的加法羣，并命 $[m]$ 表示由整数 $m>0$ 的倍数組成的子羣,这里 $x \equiv y (\mathrm{mod}\ [m])$ 与初等数論里 $x \equiv y (\mathrm{mod}\ m)$ 有同样意义,即 $x-y$ 是 m 的倍数. 設 x 是任一个整数，我們可把 x 写成 $x = qm + r$，这里 $0 \leqslant r < m$. 于是，$x \equiv r (\mathrm{mod}\ m)$. 故任一个整数与 $0, 1, \cdots, m-1$ 中一个数同余. 显然,这些数中沒有两个是同余的. 故 I 关于 $[m]$ 有 m 个陪集:

$$\overline{0} = \{0, \pm m, \pm 2m, \cdots\},$$
$$\overline{1} = \{1, 1\pm m, 1\pm 2m, \cdots\},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\overline{(m-1)} \equiv \{m-1, (m-1)\pm m, (m-1)\pm 2m, \cdots\}.$$

(2) $\mathfrak{G} = R_+$ 是实数的加法羣; $\mathfrak{H} = I_+$ 是整数子羣. 两个实数关于 I_+ 要属于同一个陪集，必須而且只須它們的差是一个整数. 故一个陪集是点的集合，这些点都以相似位置在以整数为端点的各个单位区間內.

(3) $\mathfrak{G} = S_n$, $\mathfrak{H} = A_n$. 如果 β 是偶置换，則 $\beta \in A_n$; 其逆亦眞. 如果 β 是奇置换,則不仅陪集 βA_n 里每个置换是奇置换，而且所有奇置换都含在 βA_n 里. 这因为，如果 γ 是奇置换,則 $\beta^{-1}\gamma$ 是偶置换,故 $\gamma \in \beta A_n$. 于是，我們有两个陪集：偶置换的陪

集 A_n 及奇置换的陪集.

任意两个右陪集有相同的基数；亦即有从一个陪集映照到另一个陪集上的1—1对应存在. 这因为，如果令 $x\mathfrak{H}$ 与 $y\mathfrak{H}$ 是任意两个右陪集，并考究左乘变换 $(yx^{-1})_l = x_l^{-1}y_l$；我們知道，这映照是 $\mathfrak{G}$ 到自身上的1—1映照. 如果 $xh \in x\mathfrak{H}$，則显然有

$$(xh)(yx^{-1})_l = yx^{-1}xh = yh \in y\mathfrak{H}.$$

故 $(yx^{-1})_l$ 导出 $x\mathfrak{H}$ 到 $y\mathfrak{H}$ 上的1—1映照. 因 $\mathfrak{H} = 1\mathfrak{H}$，它自身也是一个右陪集，故所有右陪集都与 $\mathfrak{H}$ 有相同的基数.

我們可以左陪集代替右陪集，重复前此討論. 此时出发点是变換羣 $\mathfrak{H}_l' = \{h_l\}$，$h \in \mathfrak{H}$. 关于子羣 $\mathfrak{H}$ 的左同余关系，我們定义为：由变換羣 $\mathfrak{H}_l'$ 所决定的同余关系，并写做 $x \equiv {}_ly \pmod{\mathfrak{H}}$ 以代替 $x \equiv y \pmod{\mathfrak{H}_l'}$. 这只是意味着，有一个元素 $h \in \mathfrak{H}$ 存在，使 $y = hx$，或等价于 $yx^{-1} \in \mathfrak{H}$. 由 x 决定的等价类是集合 $\mathfrak{H}x$，我們叫做 x 关于 $\mathfrak{H}$ 的左陪集.

由例子(习题15的第1题)可知：一个羣关于子羣 $\mathfrak{H}$ 的右陪集分解毋須与关于子羣 $\mathfrak{H}$ 的左陪集分解相一致. 但两种分解間有一个簡单的关系存在，即：由任一个右陪集里各元素的逆元素組成的集合必为一个左陪集. 这因为，$(xh)^{-1} = h^{-1}x^{-1} \in \mathfrak{H}x^{-1}$，而且当 h 历取 $\mathfrak{H}$ 的所有元素时，$h^{-1}x^{-1}$ 也历取 $\mathfrak{H}x^{-1}$ 的所有元素. 故左陪集 $\mathfrak{H}x^{-1}$ 由 $x\mathfrak{H}$ 唯一决定；亦即它与 $x\mathfrak{H}$ 里选那一个作 x 无关. 我們还知道，对应 $x\mathfrak{H} \to \mathfrak{H}x^{-1}$ 是右陪集的集合到左陪集的集合上的1—1对应，故 $\{\mathfrak{H}x\}$ 与 $\{x\mathfrak{H}\}$ 有相同的基数，这数目叫做 $\mathfrak{H}$ 在 $\mathfrak{G}$ 里的指数.

今設 $\mathfrak{G}$ 是有限羣，它的阶是 n. 令 $\mathfrak{H}$ 是一个 m 阶子羣，并記

$$\mathfrak{G} = a_1\mathfrak{H} \cup a_2\mathfrak{H} \cup \cdots \cup a_r\mathfrak{H},$$

这里，$i \neq j$ 时，$a_i\mathfrak{H} \cap a_j\mathfrak{H} = \phi$. 于是，$r$ 是 $\mathfrak{H}$ 在 $\mathfrak{G}$ 里的指数. 因 $a_i\mathfrak{H}$ 含有 m 个元素，故 $\mathfrak{G}$ 含有 mr 个元素，从而 $n = mr$. 这証明了下面的基本定理：

定理 5 (拉格兰日(Lagrange)定理). 有限羣的子羣的階數是这个羣的階數的一个因子.

因为 A_n 在 S_n 里的指数为 2，这結果指出，A_n 的阶数是 $n!/2$。拉格兰日定理的另一个重要应用是：

系 設 $\mathfrak{G}$ 是 n 階有限羣，則 $\mathfrak{G}$ 里每个元素 x 有 $x^n = 1$.

証 令 m 是 $[x]$ 的阶，则 $x^m = 1$；因为 $n = mr$，故 $x^n = 1$.

习　题 15

1. 在 S_3 里决定子羣 $\mathfrak{H} = \{1, (12)\}$ 的陪集分解.

2. 設 V 是平面上向量羣，合成用向量加法. 求証：由原点出发而終点在过 O 的一个定直綫上的向量組成一个子羣. 关于这子羣的陪集是什么？

3. 設 $\mathfrak{H}_1$ 与 $\mathfrak{H}_2$ 是 $\mathfrak{G}$ 的两个子羣. 求証：关于 $\mathfrak{H}_1 \cap \mathfrak{H}_2$ 的任一个陪集是关于 $\mathfrak{H}_1$ 的一个陪集与关于 $\mathfrak{H}_2$ 的一个陪集的交. 利用这結果来証明庞加賴 (Poincaré) 的定理：設 $\mathfrak{H}_1$ 与 $\mathfrak{H}_2$ 在 $\mathfrak{G}$ 里有有限指数，则 $\mathfrak{H}_1 \cap \mathfrak{H}_2$ 也有有限指数.

4. 法则 $x\mathfrak{H} \to \mathfrak{H}x$ 是否定义一个(单值)映照呢？

14. 不变子羣与商羣 今来决定子羣 $\mathfrak{H}$ 要适合什么条件才能使任意两个同余式模 $\mathfrak{H}$ 可以相乘，亦即才能由任意两个同余式 $x \equiv x' \pmod{\mathfrak{H}}$ 与 $y \equiv y' \pmod{\mathfrak{H}}$ 得出 $xy \equiv x'y' \pmod{\mathfrak{H}}$. 另一种探討这个条件的方法是要求：如果 $x' \in x\mathfrak{H}$ 及 $y' \in y\mathfrak{H}$，則 $x'y' \in xy\mathfrak{H}$. 由集合的乘法来說，是：对于 $\mathfrak{G}$ 里所有 x 及 y，要

$$(x\mathfrak{H})(y\mathfrak{H}) \subseteq xy\mathfrak{H} \tag{14}$$

成立. 这个条件显然等价于 $\mathfrak{H}y\mathfrak{H} \subseteq y\mathfrak{H}$ 对于所有 y 皆成立. 由 $\mathfrak{H}y\mathfrak{H} \subseteq y\mathfrak{H}$ 又可推得 $\mathfrak{H}y \subseteq y\mathfrak{H}$. 反过来，如果 $\mathfrak{H}$ 能使 $\mathfrak{H}y \subseteq y\mathfrak{H}$，因为 $\mathfrak{H}^2 = \mathfrak{H}$，就也推得

$$\mathfrak{H}y\mathfrak{H} \subseteq y\mathfrak{H}\mathfrak{H} = y\mathfrak{H}.$$

所以 $\mathfrak{H}y\mathfrak{H} \subseteq y\mathfrak{H}$ 等价于 $\mathfrak{H}y \subseteq y\mathfrak{H}$. 后者又等价于 $y^{-1}\mathfrak{H}y \subseteq \mathfrak{H}$ 也是显然的. 我們今采用这样形状的条件于下面：

定义 4. 設 $\mathfrak{H}$ 是羣 $\mathfrak{G}$ 的子羣，如果对于 $\mathfrak{G}$ 里每个 y，$y^{-1}\mathfrak{H}y \subseteq \mathfrak{H}$ 都成立，则 $\mathfrak{H}$ 叫做**不变(正规，自共軛，或类别)子羣**.

上面說明指出：$\mathfrak{H}$ 是不变子羣，必須而且只須对于 $\mathfrak{G}$ 里所有 x, y，$(x\mathfrak{H})(y\mathfrak{H}) \subseteq xy\mathfrak{H}$ 成立. 子羣 $\mathfrak{H}$ 的不变性检驗法对于元素来說就是：如果 $h \in \mathfrak{H}$，而 y 为任意元素，则 $y^{-1}hy \in \mathfrak{H}$. 因为对于所有 y，$\mathfrak{H}y \subseteq y\mathfrak{H}$，故 $\mathfrak{H}y^{-1} \subseteq y^{-1}\mathfrak{H}$. 以 y 右乘同时也左乘它，得 $y\mathfrak{H} \subseteq \mathfrak{H}y$. 故知 $\mathfrak{H}y = y\mathfrak{H}$. 所以，如果 $\mathfrak{H}$ 是不变子羣，則由任一个元素

决定的右陪集与由这个元素决定的左陪集迭合．故对于一个不变子羣的陪集分解只有一种．

設 $\mathfrak{H}$ 是不变子羣，則

$$(x\mathfrak{H})(y\mathfrak{H}) = x\mathfrak{H}y\mathfrak{H} = xy\mathfrak{H}\mathfrak{H} = xy\mathfrak{H}.$$

故 $\mathfrak{H}$ 的陪集的集合关于集合的乘法是封閉的．今証采用这样合成时，陪集的集合 $\mathfrak{G}/\mathfrak{H}$ 成一个羣．这因为，集合的乘法是可結合的，故結合律对于这样合成成立．由于 $\mathfrak{H}(x\mathfrak{H}) = x\mathfrak{H}$ 及 $(x\mathfrak{H})\mathfrak{H} = x\mathfrak{H}$，故陪集 $\mathfrak{H}$ 有恆等元素的作用．又因为

$$(x\mathfrak{H})(x^{-1}\mathfrak{H}) = \mathfrak{H} = (x^{-1}\mathfrak{H})(x\mathfrak{H}),$$

故 $x\mathfrak{H}$ 有逆元素 $x^{-1}\mathfrak{H}$．这就証明了 $\mathfrak{G}/\mathfrak{H}$ 成一个羣．由陪集的集合与所定义的合成組成的羣叫做 $\mathfrak{G}$ 关于不变子羣 $\mathfrak{H}$ 的**商(因子)羣** $\mathfrak{G}/\mathfrak{H}$．它的阶显然等于 $\mathfrak{H}$ 在 $\mathfrak{G}$ 里的指数．

例．(1) I 是整数的加法羣，$[m]$ 是整数 $m(>1)$ 的倍数所成的子羣．因为交换羣的任一个子羣显然是不变的，故 $[m]$ 是不变子羣．商羣 $I/[m]$ 是以 $\bar{1} = 1 + [m]$ 为生成元素的循环羣．(2) A_n 是 S_n 的不变子羣．这因为，如果 α 是偶置换，則对于任一个 β，$\beta^{-1}\alpha\beta$ 也是偶置换．商羣 S_n/A_n 的阶数为 2．

习　题　16

1．求証：任一个 2 阶子羣是不变的．

2．求証：$\mathfrak{H} = \{1, (12)\}$ 在 S_3 里不是不变的．

3．求証：由 $x \to x + b$ 形的变换构成的子羣在变换 $x \to ax + b$，$a \neq 0$ 所成的羣里是不变子羣．

15. 羣的同态　同构及同构的羣的概念按下面所述的方式拓广，內容就更見丰富．这种拓广是将前此定义中弃去 1—1 的要求，故有下面的基本定义．

定义 5.　設从羣 $\mathfrak{G}$ 到羣 $\mathfrak{G}'$ 內的映照 η 有性質

$$(xy)\eta = (x\eta)(y\eta),$$

則 η 叫做**同态**．如果 η 是 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 上的一个同态，則 $\mathfrak{G}'$ 叫做 $\mathfrak{G}$ 的**同态象**．

同态的一个重要例子，可由取 $\mathfrak{G}$ 关于它的一个不变子羣 $\mathfrak{H}$ 的商羣 $\mathfrak{G}/\mathfrak{H}$ 而得到．由定义，在 $\mathfrak{G}/\mathfrak{H}$ 里

$$(x\mathfrak{H})(y\mathfrak{H}) = (xy)\mathfrak{H}.$$

所以，如果我們把 $\mathfrak{G}$ 的元素 x 映照到它的陪集 $x\mathfrak{H}$ 里，则得 $\mathfrak{G}$ 到 $\mathfrak{G}/\mathfrak{H}$ 上的一个同态. 因此，$\mathfrak{G}$ 的任一个商羣是 $\mathfrak{G}$ 的一个同态象.

必須指出，上面的定义沒有要求 η 是到 $\mathfrak{G}'$ 上的映照. 如果 η 是 1—1 的，則叫它做 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 內的同构. 以前我們只就 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 上的同构及同构羣来討論. 現在考究同态的一些具体例子.

例. (1) 令 $\mathfrak{G} = R_+$ 是实数的加法羣，并令 $\mathfrak{G}' = U$ 是絕对值为 1 的复数乘法羣. 因为 $e^{i(\theta_1+\theta_2)} = e^{i\theta_1}e^{i\theta_2}$，而且 $\mathfrak{G}'$ 的每个元素形状为 $e^{i\theta}$，所以 $\theta \to e^{i\theta}$ 是 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 上的一个同态. 这映照不是同构的，并且实际上也容易知道，这些羣不是同构的(习題 17 的第 3 題). (2) 令 $\mathfrak{G} = V$ 是平面上向量 (α, β) 的羣，它用熟知的合成 $(\alpha, \beta) + (\alpha', \beta') = (\alpha + \alpha', \beta + \beta')$，則 $(\alpha, \beta) \to \alpha$ 是 V 到 R_+ 上的同态. (3) 令 $\mathfrak{G}$ 是对称羣 S_n，并按置换 $\tau(\in S_n)$ 是偶的或是奇的，而把 τ 映照到数 1 或 -1 上. 在任一种情形下，我們記它的象为 $\chi(\tau)$. 則 $\chi(\tau\tau') = \chi(\tau)\chi(\tau')$. 于是，$\tau \to \chi(\tau)$ 是 S_n 到数 $1, -1$ 的乘法羣上的同态. (4) 考究整数的加法羣 I_+ 与任一个羣 $\mathfrak{G}$. 令 a 是 $\mathfrak{G}$ 的一定元素，則映照 $n \to a^n$，$n \in I_+$，适合 $a^{m+n} = a^m a^n$. 故它是 I_+ 到 $\mathfrak{G}$ 內的一个同态.

接着我們要导出同态的一些初等性质. 先述下面的：

定理 6. $\mathfrak{G}$ 到 $\mathfrak{G}'$ 內的一个同态 η 的像 $\mathfrak{G}\eta$ 是 $\mathfrak{G}'$ 的一个子羣.

証 因为 $(x\eta)(y\eta) = (xy)\eta$，故 $\mathfrak{G}\eta$ 在 $\mathfrak{G}'$ 里的合成下封閉. 又因为 $(1\eta)(1\eta) = 1\eta$，故 1η 是 $\mathfrak{G}'$ 的恆等元素 $1'$. 最后，因为 $(x\eta)(x^{-1}\eta) = 1\eta = 1'$，可見 $(x\eta)^{-1} = x^{-1}\eta$ 是属于 $\mathfrak{G}\eta$.

次考究 $\mathfrak{G}$ 的元素 k 能使 $k\eta = 1'$ 的所有元素的集合 $\mathfrak{K}$; 这是 $\mathfrak{G}'$ 的恆等元素 $1'$ 的逆象集合 $\eta^{-1}(1')$. 因为 $1\eta = 1'$，所以 $1 \in \mathfrak{K}$. 故若 $\mathfrak{K} \neq 1$，則 η 不是 1—1 的. 另一方面，我們要証：如果 $\mathfrak{K} = 1$，則 η 是一个同构. 这因为，如果 $a\eta = b\eta$，則

$$(a^{-1}b)\eta = (a^{-1}\eta)(b\eta) = (a\eta)^{-1}(b\eta) = 1'.$$

故 $a^{-1}b = 1$，而 $a = b$. 次証

定理 7. 設 η 是 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 內的一个同态，則 $\mathfrak{G}'$ 的恆等元素的逆像 $\mathfrak{K} = \eta^{-1}(1')$ 是 $\mathfrak{G}$ 的一个不变子羣.

証 我們知道，$1 \in \mathfrak{K}$. 如果 $k_1, k_2 \in \mathfrak{K}$，則

$$(k_1k_2)\eta = (k_1\eta)(k_2\eta) = 1'1' = 1'.$$

故 $k_1k_2 \in \mathfrak{K}$. 又設 $k \in \mathfrak{K}$，則 $k^{-1}\eta = (k\eta)^{-1} = 1'^{-1} = 1'$，而 $k^{-1} \in \mathfrak{K}$. 这証明 $\mathfrak{K}$ 是一个子羣. 最后，設 a 是 $\mathfrak{G}$ 里任意元素，而 $k \in \mathfrak{K}$，則

$$(a^{-1}ka)\eta = (a^{-1}\eta)(k\eta)(a\eta) = (a\eta)^{-1}1'(a\eta) = 1'.$$

故 $a^{-1}ka \in \mathfrak{K}$. 于是, $\mathfrak{K}$ 是不变子羣.

羣 $\mathfrak{K} = \eta^{-1}(1')$ 叫做同态 η 的**核**.

习 題 17

1. 就前面各个例子决定同态核.

2. 求証定理 6 的下面拓广:令 $\mathfrak{G}$ 是一个羣, 而 $\mathfrak{G}'$ 是定义有合成 $a'b'$ 的任一个集合. 假設 η 是 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 内的任一个映照, 使 $(xy)\eta = (x\eta)(y\eta)$, 則象 $\mathfrak{G}\eta$ 对于 $\mathfrak{G}'$ 里所定义的合成来説,成一个羣.

3. 求証:羣 R_+ 与例 1 的羣 U 不同构.

4. 令 $\mathfrak{G}$ 是映照 $x \to ax + b$ 所成的变换羣,这里 a 与 b 是实数,而 $a \neq 0$. 求証:把上述的变换与实数 a 联結起来的对应是 $\mathfrak{G}$ 到 R^* 上的一个同态. 它的核是什么?

5. 求証:如果 k 是一个整数, 則映照 $e^{i\theta} \to e^{ki\theta}$ 是 U 到它自身上的一个同态. 决定它的核.

16. 关于羣的同态基本定理 我們知道, $x \to \bar{x} = x\mathfrak{H}$ 是由羣 $\mathfrak{G}$ 到它关于不变子羣 $\mathfrak{H}$ 的商羣 $\bar{\mathfrak{G}} = \mathfrak{G}/\mathfrak{H}$ 上的一个同态. 这样的同态叫做 $\mathfrak{G}$ 到 $\bar{\mathfrak{G}}$ 上的**自然同态**; 此后記作 ν. ν 的核, 亦即能使 $a\nu \equiv a\mathfrak{H} = \mathfrak{H}$ 的元素 a 的集合,显然就是給定的不变子羣 $\mathfrak{H}$.

次設 η 是 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 内的一个同态, 而 ρ 是 $\mathfrak{G}'$ 到 $\mathfrak{G}''$ 内的一个同态. 由定义立知, $\eta\rho$ 是 $\mathfrak{G}$ 到 $\mathfrak{G}''$ 内的一个同态. 其特款是: 如果 ν 是 $\mathfrak{G}$ 到 $\bar{\mathfrak{G}} = \mathfrak{G}/\mathfrak{H}$ 上的自然同态,而 $\bar{\eta}$ 是 $\bar{\mathfrak{G}}$ 到另一个羣 $\mathfrak{G}'$ 内的一个同态,則积 $\nu\bar{\eta}$ 是 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 内的一个同态,它的核显然含有 $\mathfrak{H}$.

反过来,令 η 是 $\mathfrak{G}$ 到另一羣 $\mathfrak{G}'$ 内的一个同态,并令 $\mathfrak{H}$ 是 $\mathfrak{G}$ 的一个不变子羣, 它含在核 $\mathfrak{K} = \eta^{-1}(1')$ 内. 命 a 与 b 是关于 $\mathfrak{H}$ 的同一个陪集里的两个元素,則 $b = ah$, $h \in \mathfrak{H}$, 而且

$$b\eta = (a\eta)(h\eta) = (a\eta)1' = a\eta.$$

这証明了 $a\mathfrak{H} \to a\eta$ 定义从 $\bar{\mathfrak{G}} = \mathfrak{G}/\mathfrak{H}$ 到 $\mathfrak{G}'$ 内的一个单值映照. 我們把它記作 $\bar{\eta}$. 因为

$$[(a\mathfrak{H})(b\mathfrak{H})]\bar{\eta} = (ab\mathfrak{H})\bar{\eta} = (ab)\eta$$
$$= (a\eta)(b\eta) = ((a\mathfrak{H})\bar{\eta})((b\mathfrak{H})\bar{\eta}),$$

所以 $\bar{\eta}$ 是一个同态, 叫做 $\bar{\mathfrak{G}}$ 到 $\mathfrak{G}'$ 内的**导出同态**. 显然, $a\nu\bar{\eta} = (a\mathfrak{H})\bar{\eta} = a\eta$; 故給定的同态允許因子分解为 $\eta = \nu\bar{\eta}$.

次設 $(a\mathfrak{H})\bar{\eta} = 1'$, 則 $a\eta = 1'$, 而 $a \in \mathfrak{K}$. 反过来也是成立. 故知, $\bar{\eta}$ 的核是如 $k\mathfrak{H}$ 形的陪集的全部 $\mathfrak{K}/\mathfrak{H}$, 这里 $k \in \mathfrak{K}$. 由此可

得的一个結果是：$\bar{\eta}$ 为 1—1 的必須而且只須 $\mathfrak{K} = \mathfrak{H}$. 这就証明了重要的下述定理.

定理 8. 令 η 是 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 内的一个同态，並令 $\mathfrak{H}$ 是 $\mathfrak{G}$ 的一个不变子羣，$\mathfrak{H} \subseteq \mathfrak{K} = \eta^{-1}(1')$. 則 $a\mathfrak{H} \to a\eta$ 是 $\bar{\mathfrak{G}} = \mathfrak{G}/\mathfrak{H}$ 到 $\mathfrak{G}'$ 内的一个同态 $\bar{\eta}$，並且 $\eta = \nu\bar{\eta}$，这里 ν 是 $\mathfrak{G}$ 到 $\bar{\mathfrak{G}}$ 上的自然同态. $\bar{\eta}$ 是一个同構，必須而且只須 $\mathfrak{K} = \mathfrak{H}$.

今若把上面的討論用于特殊情况：η 是 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 上的一个同态. 如果 $\mathfrak{K}$ 是核，即知 $\bar{\mathfrak{G}} = \mathfrak{G}/\mathfrak{K}$ 到 $\mathfrak{G}'$ 上的导出映照 $\bar{\eta}$ 是一个同构. 故 $\bar{\mathfrak{G}} \cong \mathfrak{G}'$. 这結果与第一段結果合并起来，証明了

关于羣的同态基本定理 $\mathfrak{G}$ 的任一个商羣是 $\mathfrak{G}$ 的一个同态像. 反过来，如果 $\mathfrak{G}'$ 是 $\mathfrak{G}$ 的一个同态像，則 $\mathfrak{G}'$ 与 $\mathfrak{G}$ 的一个商羣是同構的.

我們用这个定理再一次地导出循环羣的一部分理論，作为这个定理的功用的說明. 令 $\mathfrak{G} = [a]$ 是循环羣，a 为生成元素，則可見 $n \to a^n$ 是 I_+ 到 $\mathfrak{G}$ 上的一个同态. 于是，$\mathfrak{G} \cong I_+/\mathfrak{H}$，这里 $\mathfrak{H}$ 作为核，是 I_+ 的一个子羣. 至此，我們使用 I_+ 的子羣决定法，即得 $\mathfrak{H} = 0$，或 $\mathfrak{H} = [m]$，这里 $m > 0$. 如果 $\mathfrak{H} = 0$，映照 $n \to a^n$ 是一个同构，而有 $\mathfrak{G} \cong I_+$. 否則，$\mathfrak{G} \cong I_+/[m]$ 是一个 m 阶羣. 由此可見，同阶的任意两个循环羣都是同构的.

习　　題　18

1. 求証：$R_+/[2\pi] \cong U$，这里 R_+ 及 U 的意义与 §15 的例 1 同，而 $[2\pi]$ 是由 2π 生成的循环羣.

2. 令 $[x]$ 是 s 阶循环羣，$[y]$ 是 t 阶循环羣. 令 η 表 $[x]$ 到 $[y]$ 内的一个同态，使 $x\eta = y^k$. 求証：这个映照存在，必須而且只須 sk 是 t 的倍数. 設 $sk = mt$，求証：η 是一个同构必須而且只須 $(s, m) = 1$.

17. 自同态，自同构，羣的心　一个羣到它自身内的同态叫做自同态. 一个羣到它自身上的同构叫做自同构. 自同态的积是一个自同态. 故一个羣 $\mathfrak{G}$ 的自同态的集合 $\mathfrak{E}$ 是集合 $\mathfrak{G}$ 里单值映照所成半羣的一个子半羣. 显然，恆等变换是一个自同态，故半羣 $\mathfrak{E}$ 含有一个恆等元素.

今考究羣 $\mathfrak{G}$ 的自同构的集合 $\mathfrak{A}$. 則 $\mathfrak{A}$ 是由 $\mathfrak{E}$ 的单位元素組

成的．这因为，如果 α 是 $\mathfrak{E}$ 里一个单位元素，则 α^{-1} 存在；故 α 是 $\mathfrak{G}$ 到它自身上的 1—1 变换．反过来，如果 α 是一个自同构，则它的逆元素 α^{-1} 也是一个自同构．这因为，

$$(xy)\alpha^{-1} = ((x\alpha^{-1}\alpha)(y\alpha^{-1}\alpha))\alpha^{-1}$$
$$= (((x\alpha^{-1})(y\alpha^{-1}))\alpha)\alpha^{-1} = (x\alpha^{-1})(y\alpha^{-1}).$$

所以，α 在 $\mathfrak{E}$ 里有一个逆元素．这也証明了，$\mathfrak{A}$ 是 $\mathfrak{G}$ 里一个变换羣；我們叫它做 $\mathfrak{G}$ 的**自同构羣**．

設 a 是一个固定元素，則映照

(15) $$C_a: x \to a^{-1}xa$$

是 $\mathfrak{G}$ 的一个自同构．这因为

$$a^{-1}(xy)a = (a^{-1}xa)(a^{-1}ya),$$

而且 C_a 是 $\mathfrak{G}$ 到它自身上的 1—1 变换的緣故．后者是容易証驗的，事实上，如果我們注意到

(16) $$C_a = a_r a_l^{-1} = a_l^{-1} a_r,$$

則 1—1 性就明显了；这里，a_r 与 a_l 分别表示由 a 决定的右乘与左乘变换．自同构 C_a 叫做由元素 a 决定的**內自同构**．

今来証明：內自同构的集合 $\mathfrak{J}$ 成自同构羣 $\mathfrak{A}$ 的一个不变子羣．令 C_{a_1} 与 C_{a_2} 是內自同构，則

$$xC_{a_1}C_{a_2} = a_2^{-1}a_1^{-1}xa_1a_2 = (a_1a_2)^{-1}x(a_1a_2) = xC_{a_1a_2},$$

故

(17) $$C_{a_1a_2} = C_{a_1}C_{a_2}.$$

这个方程指出：对应 $a \to C_a$ 是 $\mathfrak{G}$ 到它的自同构羣的一个同态．故(由定理 6)知，象集合 $\mathfrak{J}$ 是 $\mathfrak{A}$ 的一个子羣．今令 α 是任一个自同构，并考究积 $\alpha^{-1}C_a\alpha$．因为

$$x\alpha^{-1}C_a\alpha = (a^{-1}(x\alpha^{-1})a)\alpha = (a^{-1}\alpha)x(a\alpha)$$
$$= (a\alpha)^{-1}x(a\alpha) = xC_{a\alpha},$$

故

(18) $$\alpha^{-1}C_a\alpha = C_{a\alpha}$$

是內自同构．这証明了 $\mathfrak{J}$ 的不变性．商羣 $\mathfrak{A}/\mathfrak{J}$ 叫做羣 $\mathfrak{G}$ 的**外自同构羣**．

再就 $\mathfrak{G}$ 到 $\mathfrak{I}$ 上的同态 $a \to C_a$ 来說,这映照的核 $\mathfrak{C}$ 是元素 c 的集合,它使 $C_c=1$. 故 $c \in \mathfrak{C}$ 必须而且只须对于所有 x, $c^{-1}xc = x$, 或等价于

$$(19) \qquad cx = xc.$$

$\mathfrak{C}$ 叫做羣 $\mathfrak{G}$ 的心. 由定理 7 或直接地知道: $\mathfrak{C}$ 是一个不变子羣. 又由同态基本定理得, $\mathfrak{I} \cong \mathfrak{G}/\mathfrak{C}$. 綜合这些結果,得下面定理:

定理 9. 內自同構的集合 $\mathfrak{I}$ 是自同構羣的一个不变子羣, 並且 $\mathfrak{I} \cong \mathfrak{G}/\mathfrak{C}$, 这里 $\mathfrak{C}$ 是羣的心.

习 題 19

1. 求証:映照 $a \to a^{-1}$ 是一个自同构,必須而且只須 $\mathfrak{G}$ 是交換羣.
2. 求証:如果 k 是一个整数,而 $\mathfrak{G}$ 是交換羣,則 $a \to a^k$ 是一个自同态.
3. 决定任一个循环羣的自同构羣.
4. 决定对称羣 S_3 的自同构羣.
5. 由自同构羣及右乘变换羣生成的变换羣 $\mathfrak{H}$, 叫做羣 $\mathfrak{G}$ 的全形羣. 求証:
   (1) $\mathfrak{H}$ 包含所有左乘变换.
   (2) $\mathfrak{H}$ 的任一个元素必能而且只能有一个方法写做一个自同构 α 与一个右乘变换 a_r 的积 αa_r.
   (3) 如果 $\mathfrak{G}$ 是有限羣,則 $\mathfrak{H}$ 的阶是 $\mathfrak{G}$的阶与 $\mathfrak{A}$ 的阶的积.

18. 共軛类 如果 $\mathfrak{G}$ 的元素 x 与 y 对于由变換羣 $\mathfrak{I}$ 决定的同余关系成等价, 亦即 $\mathfrak{G}$ 里存在一个 a, 使$a^{-1}xa = y$, 我們說,这两个元素成共軛. 由羣 $\mathfrak{I}$ 决定的各个传递集合叫做羣 $\mathfrak{G}$ 的共軛类. 由元素 c 决定的共軛类仅含一个元素必須而且只須 c 是属于羣的心.

今来决定对称羣 S_n 的共軛类,借以說明这些观念. 首先我們知道,如果 α 是置換

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ 1\alpha & 2\alpha & \cdots & n\alpha \end{pmatrix},$$

而 β 是任意置換,則 $\beta^{-1}\alpha\beta$ 把 1β 映照到 $1\alpha\beta$, 故 $\beta^{-1}\alpha\beta$ 可由記号

$$\begin{pmatrix} 1\beta & 2\beta & \cdots & n\beta \\ 1\alpha\beta & 2\alpha\beta & \cdots & n\alpha\beta \end{pmatrix}$$

表出. 所以,如果

$$(20) \qquad \alpha = (i_1 i_2 \cdots i_r)(j_1 j_2 \cdots j_s) \cdots (l_1 l_2 \cdots l_u),$$

則

(21) $$\beta^{-1}\alpha\beta=(i_1\beta i_2\beta\cdots i_r\beta)\cdots(l_1\beta l_2\beta\cdots l_u\beta).$$

我們可假定 $r\geqslant s\geqslant\cdots\geqslant u$，而且所有数目都出現于 (20) 里。于是，$r+s+\cdots+u=n$. 按这个方式，我們可把适合

(22) $$r\geqslant s\geqslant\cdots\geqslant u,\quad r+s+\cdots+u=n$$

的正整数 $r, s, \cdots, u$ 的集合与 α 联結起来. 方程 (21) 指出，α 与 α' 在 S_n 里共軛必須而且只須与这两个置换連带的集合 $r, s, \cdots, u$ 必相同. 一組适合 (22) 的整数叫做 n 的一个划分. 于是，S_n 里的共軛类与 n 的划分間有一个 1—1 对应. 共軛类的个数与 n 的不同划分的个数 $p(n)$ 相同. 函数 $p(n)$ 是一个重要的算术函数，它的前几个数值是

$$p(2)=2,\ p(3)=3,\ p(4)=5,\ p(5)=7,\ p(6)=11.$$

由 (21) 还易知：如果 $r>1$ 而 $n>2$，則可取 β 使 $\beta^{-1}\alpha\beta\neq\alpha$. 故若 $\alpha\neq1$，則有一个 β 存在，使 $\beta\alpha\neq\alpha\beta$. 这証明了 S_n $(n>2)$ 的心是恆等元素.

习　题　20

1. 求証：如果 $\mathfrak{G}$ 是一个有限置换羣，則由 $\mathfrak{G}$ 决定的任一个传递集合里的元素个数是羣的阶数的一个因子.

(提示：如果 i 是集合 $S=\{1,2,\cdots,n\}$ 里任一个数目，則 $\mathfrak{G}$ 里使 i 不变的变换 α 的集合是一个子羣 $\mathfrak{H}$. 証明：含有 i 的传递集合里的元素可与 $\mathfrak{H}$ 的左陪集成 1—1 对应. 然后証明，传递集合里元素的个数是 $\mathfrak{H}$ 在 $\mathfrak{G}$ 里的指数.)

2. 求証：在一个有限羣 $\mathfrak{G}$ 的任一个共軛类里，元素的个数是 $\mathfrak{G}$ 的阶数的一个因子.

3. 求証：阶数是素数幂的羣的心所含元素多于 1 个.

第 二 章

环.整区及域

本章开始討論代数系的第二种重要类型,叫做环.我們即将知道,环是带有适当限制的两种二元合成的集合. 环論与羣論不同.羣論只有一个根源,即研究关于积合成的 1—1 变换的集合;而环論是从若干专門理論汇合出来. 因此会多少地显出不能象羣論的連貫. 本章介紹整区、除环、域、理想、差环、同构、同态及反同构等基本概念. 我們还介紹一些重要的特殊环的例子,象陣环及四維数环. 最后,我們就环論上証明与羣論里凯莱定理相类似的定理.

1. 定义及例

定义 1. 环是由一个集合 $\mathfrak{A}$ 及 $\mathfrak{A}$ 里叫做加法与乘法的两个二元合成組織而成,使

1. $\mathfrak{A}$ 带着加法(+)是一个交换羣.
2. $\mathfrak{A}$ 带着乘法(·)是一个半羣.
3. 分配律

D $\quad a(b+c)=ab+ac,\quad (b+c)a=ba+ca$

成立.

故在假設 1 及 2 下,含有 $a+b$ 及 $ab\in\mathfrak{A}$,且适合下面各个条件:

A_1. $\qquad (a+b)+c=a+(b+c)$.

A_2. $\qquad a+b=b+a$.

A_3. 有一个元素 0 存在,使 $a+0=a=0+a$.

A_4. 对于每个 a,存在一个負元素 $-a$,使 $a+(-a)=0=-a+a$.

M. $$(ab)c=a(bc).$$

代数系 $\mathfrak{A}, +$ 叫做环的**加法羣**,而代数系 $\mathfrak{A}, \cdot$ 叫做环的**乘法半羣**.

例. (1) 整数的集合 I, 用通常的加法及乘法.我們在引論里已說过这是一个环. (2) 有理数的集合 R_0, 用通常的加法及乘法. 这个环的严格定义在下一章給出. (3) 实数的集合 R, 用通常的加法及乘法. (4) 如 $m+n\sqrt{2}$ 形的实数的集合 $I[\sqrt{2}]$, 这里 m 与 n 是整数, 用通常的加法及乘法. 显然 $I[\sqrt{2}]$ 里两个数的和与差属于这集合內. 又

$$(m+n\sqrt{2})(m'+n'\sqrt{2})=(mm'+2nn')+(mn'+nm')\sqrt{2},$$

故 $I[\sqrt{2}]$ 对于乘法封閉. 由此易知,这个代数系是一个环(参看 §5 里子环的討論). (5) 如 $a+b\sqrt{2}$ 形的实数的集合 $R_0[\sqrt{2}]$, 这里 a 与 b 是有理数, 用通常的加法及乘法. (6) 复数的集合 C, 用通常的加法及乘法. (7) 如 $m+n\sqrt{-1}$ 形的复数的集合 $I[\sqrt{-1}]$,这里 m 与 n 是整数,用通常加法及乘法. 这例子与 (4) 相似. (8) 在区間 $[0, 1]$ 上实值連續函数的集合 Γ, 这里

$$(f+g)(x)=f(x)+g(x), \quad (fg)(x)=f(x)g(x).$$

(9) 由两个元素 0, 1 組成的集合,其加法表及乘法表是

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

习 题 21

1. 令 A 是 $(-\infty, \infty)$ 上所有实值函数的集合. 求証: A 对于通常加法是一个羣, 而对于 $f\cdot g(x)=f(g(x))$ 是一个半羣. A 关于这两个合成是否成一个环呢?

2. 求証:如果在三个元素 0, 1, 2 的集合里定义加法及乘法如下表,

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

則它成一个环.

环的若干初等性質都由环关于加法是一个羣而关于乘法是一个半羣的事实引出. 例如,我們有

$$-(a+b)=-a-b\equiv -a+(-b).$$

又若对于整数 n 如前定义 na, 則关于倍数法則

$$n(a+b)=na+nb,$$

$$(m+n)a = ma + na,$$
$$(nm)a = n(ma)$$

成立. 再則拓广的結合律对于加法及乘法都成立，而拓广的交换律对于加法成立. 由分配律还可得出若干其他結果. 首先，就 m 及 n 使用归納法，得出拓广

$$(a_1 + a_2 + \cdots + a_m)(b_1 + b_2 + \cdots + b_n)$$
$$= a_1b_1 + a_1b_2 + \cdots + a_1b_n + a_2b_1 + a_2b_2$$
$$+ \cdots + a_2b_n + \cdots + a_mb_1 + \cdots + a_mb_n,$$

或

$$\left(\sum_1^m a_i\right)\left(\sum_1^n b_j\right) = \sum_{i=1,\ j=1}^{m,n} a_ib_j.$$

其次，对于所有 a 有

$$a0 = 0 = 0a,$$

这因为 $a0 = a(0+0) = a0 + a0$，以 $-a0$ 加于两端得 $a0 = 0$. 仿此得 $0a = 0$. 由方程

$$0 = 0b = (a + (-a))b = ab + (-a)b,$$

得

$$(-a)b = -ab.$$

同理得 $a(-b) = -ab$. 故

$$(-a)(-b) = -a(-b) = -(-ab) = ab.$$

习　　題　22

1. 求証：$a(b-c) = ab - ac$.
2. 求証：对于任一个整数 n，$n(ab) = (na)b = a(nb)$.
3. 令 $\mathfrak{A}$ 是一个代数系，适合环的所有条件，只把加法的交换性除外. 如果 $\mathfrak{A}$ 含有一个元素 c，它可以左相消，亦即如果 $ca = cb$，則 $a = b$，求証：$\mathfrak{A}$ 是一个环.

設 a 与 b 可交换，亦即 $ab = ba$，則 a 的冪可与 b 的冪交换. 我們由归納法可証重要的二項定理：

(1)　$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + b^n,$

这里 $\binom{n}{i}$ 是一个整数，由公式

$$(2) \qquad \binom{n}{i} = \frac{n!}{i!(n-i)!}$$

决定．这因为，$n=1$ 时，(1) 显然成立．今假定

$$(3) \qquad (a+b)^r = \sum_{k=0}^{r} \binom{r}{k} a^k b^{r-k}.$$

在使用 $0!=1$ 的規定下，(3) 就与 (1) 在 $n=r$ 时的結果一致．今以 $a+b$ 乘 (3) 的两端，得

$$(a+b)^{r+1} = \sum_{k=0}^{r} \binom{r}{k} a^{k+1} b^{r-k} + \sum_{k=0}^{r} \binom{r}{k} a^k b^{r-k+1}.$$

如果 $k \neq 0, r+1$，則这方程右端的項 $a^k b^{r-k+1}$ 的系数是

$$\binom{r}{k} + \binom{r}{k-1} = \frac{r!}{k!(r-k)!} + \frac{r!}{(k-1)!(r-k+1)!}$$

$$= \frac{r!(r-k+1) + r!k}{k!(r-k+1)!}$$

$$= \frac{(r+1)!}{k!(r-k+1)!} = \binom{r+1}{k}.$$

故知 (1) 在 $n=r+1$ 时也成立，而証明完成．

2. 环的类型 如果我們給乘法半羣添上条件，則得不同类型的环．譬如，如果环 $\mathfrak{A}$ 的乘法半羣是可交換的，$\mathfrak{A}$ 就叫做**交換环**．如果环 $\mathfrak{A}$ 的乘法半羣里含有恆等元素，$\mathfrak{A}$ 就叫做**带恆等元素环**．如果这样一个元素存在，則必是唯一的．上面所举各例都是可交換且带恆等元素的．不带恆等元素的环的一个例子是偶整数的集合．非交換环的例子将于 §§4,5 里揭出．如果恆等元素 $1=0$，則任一个 $a=a1=a0=0$，故 $\mathfrak{A}$ 只含有一个元素．換句話說，如果 $\mathfrak{A} \neq 0$，則 $1 \neq 0$．

如果一个环里非零元素的集合 $\mathfrak{A}^*$ 决定乘法半羣的一个子半羣，这只是說，如果 $\mathfrak{A}$ 里 $a \neq 0$，$b \neq 0$，則 $ab \neq 0$，这样环叫做**整区**．上面例子中，除 (8) 外，都属于这种类型．另一方面，我們可从 (8) 里取两个元素

$$f(x)=\begin{cases}0, & \left(0\leqslant x\leqslant \frac{1}{2}\right)\\ x-\frac{1}{2} & \left(\frac{1}{2}<x\leqslant 1\right)\end{cases}$$

$$g(x)=\begin{cases}-x+\frac{1}{2} & \left(0\leqslant x\leqslant \frac{1}{2}\right)\\ 0 & \left(\frac{1}{2}<x\leqslant 1\right).\end{cases}$$

則 $f\neq 0$（0 是常数函数），并且 $g\neq 0$，但 $fg=0$. 故 $[0,1]$ 上連續函数的环不是一个整区.

設 a 是环 $\mathfrak{A}$ 的一个元素，如果存在一个 $b\neq 0$，使 $ab=0$ $(ba=0)$，則 a 叫做 $\mathfrak{A}$ 里的左(右)零因子. 如果 $\mathfrak{A}$ 里元素不只一个，則元素 0 显然是左及右零因子. 如果 $a\neq 0$ 是左零因子，而对于 $b\neq 0$ 有 $ab=0$，則 b 是一个非零的右零因子. 故由定义显然知道：环是一个整区必須而且只須它不含有非零的零因子.

还应指出，环是一个整区必須而且只須乘法的狹义相消律成立. 狹义相消律是說：如果 $a\neq 0$，而 $ab=ac$，可推得 $b=c$；又 $a\neq 0$，而 $ba=ca$，可推得 $b=c$. 因此，假設 $\mathfrak{A}$ 是一个整区，并令 a,b,c 是 $a\neq 0$ 而能使 $ab=ac$ 的元素，則 $a(b-c)=0$；于是，$b-c=0$，而 $b=c$. 仿此可証右相消律也成立. 反过来，令 $\mathfrak{A}$ 是左相消律能成立的任一个环. 令 $ab=0$，$a\neq 0$；則 $ab=a0$，故 $b=0$. 于是，$\mathfrak{A}$ 是一个整区.

如果一个环不只含一个元素，且非零元素的集合 $\mathfrak{A}^*$ 成乘法半羣的子羣，这样的环叫做除环（拟域，斜域，s–域）[1]. 故若 $\mathfrak{A}$ 是一个除环，則 $\mathfrak{A}^*$ 含有一个恆等元素 1. 因 $10=0=01$，故 1 也是整个环的恆等元素. 于是，除环含有一个恆等元素. 又若 $a\neq 0$，則 $\mathfrak{A}$ 里存在一个元素 a^{-1}，使 $aa^{-1}=1=a^{-1}a$. 例 (2)，(3)，(5)，(6) 及 (9) 都是除环，而且乘法是可交換的. 具有这样性質的除环叫做域. 我們于 §5 中給出非交換除环的例子.

---

1) 除环也譯作体——譯者注.

由定义显然可知，任一个除环是一个整区．在另一方面，因整数环 I 是一个整区，但不是一个除环，故逆定理不成立．設在除环 $\mathfrak{A}$ 里，$a \neq 0$，則方程 $ax = b$ 在 $\mathfrak{A}$ 里有一个解 $x = a^{-1}b$．由狹义相消律知，这是方程的唯一解．同理，$ya = b$ 必有而且只有一个解，即 $y = ba^{-1}$．

今令 $\mathfrak{A}$ 是带恆等元素 $1 \neq 0$ 的任一个环．由半羣的討論知，$\mathfrak{A}$ 的乘法半羣中单位元素的全部 $\mathfrak{U}$ 是这个半羣的一个子羣．这就是說，单位元素的积是一个单位元素，1 是一个单位元素，而单位元素的逆元素是一个单位元素．我們把 $\mathfrak{U}$ 叫做环 $\mathfrak{A}$ 的**单位元素羣**．例如，I 的单位元素羣由数 1 与 -1 組成．我們易知，环 $\mathfrak{A}$ 是一个除环必須而且只須：(1) $\mathfrak{A}$ 含有一个恆等元素 $\neq 0$，及 (2) $\mathfrak{A}$ 的单位元素羣是非零元素的集合 $\mathfrak{A}^*$．

习　题　23

1．求証：如果 a 是带恆等元素环里一个单位元素，則 $-a$ 也是单位元素．証明：$(-a)^{-1} = -a^{-1}$．

2．求証：习題 21 的第 2 題里所給的代数系是一个域．

3．求証：任一个有限整区是一个除环．

4．求証：如果一个整区 $\mathfrak{A}$ 有一个同势元素 $e \neq 0$ $(e^2 = e)$，則 e 是 $\mathfrak{A}$ 的恆等元素．

5．如果环里一个元素 z 适合 $z^n = 0$，这元素叫做**无势元素**[1]．求証：整区的唯一无势元素是 $z = 0$．

6．如果一个环只有左恆等元素 1_l，求証：1_l 是(双側)恆等元素．

7．令 u 是带恆等元素环的一个元素，它有一个右逆元素．求証：下面关于 u 的各个条件都是等价的：

(1) u 拥有不只一个的右逆元素，

(2) u 不是一个单位元素，

(3) u 是一个左零因子．

8．卡浦兰斯基 (Kaplansky) 定理：如果带恆等元素环的一个元素拥有不只一个右逆元素，則它有无数个右逆元素．

***3．拟正則性，圓合成**　我們将要看到，带恆等元素环的单位元素羣会給出羣的有趣例子．这里値得注意的是，在对于不拥有恆等元素的任意环里也有类似于单位元素羣的概念．要得出这个

---

1) 无势元素也譯作冪零元素．——著者注．

类似概念，先假定$\mathfrak{A}$拥有一个恆等元素. 如果a是$\mathfrak{A}$的一个元素，它有右逆元素b，我們令$a=1-z, b=1-w$，得

$$1=ab=(1-z)(1-w)=1-z-w+zw.$$

所以关于z及w的条件是

$$z+w-zw=0.$$

由于这个条件不含有恆等元素，故可应用于任意环. 因此，如果$\mathfrak{A}$里对于元素z有一个元素w存在，使$z+w-zw=0$ ($z+w-wz=0$)，則z叫做**右(左)拟正則元素**，而w叫做z的**右(左)拟逆元素**.

要更好地了解拟正則性的概念，可作如下考究. 令$\mathfrak{A}$是一个任意环. 在$\mathfrak{A}$里以公式

$$a\circ b=a+b-ab$$

来定义二元合成，叫它做$\mathfrak{A}$里**圓合成**. 我們可直接驗証它是可結合的. 故$\mathfrak{A},\circ$是一个半羣. 显然$a\circ 0=a=0\circ a$，故0在$\mathfrak{A},\circ$里有恆等元素的作用. 至此显然知，成**拟正則**(=左及右拟正則)元素的集合$\mathfrak{Q}$就是$\mathfrak{A},\circ$的单位元素的集合. 故$\mathfrak{Q},\circ$是一个羣.

任意环里的羣$\mathfrak{Q},\circ$与带恆等元素环的单位元素羣类似. 事实上，如果$\mathfrak{A}$有一个恆等元素，則$\mathfrak{U}$与$\mathfrak{Q}$成同构. 这因为，映照$z\to 1-z$易知是$\mathfrak{Q}$到$\mathfrak{U}$上的一个同构.

习 題 24

1. 如果e是同势元素，求証: $e\circ e=e$. 于是，求証: 如果e是右拟正則元素，則$e=0$.
2. 求証:任一个无势元素属于$\mathfrak{Q}$.
3. 求証卡浦兰斯基关于一个除环的特性的定理: 一个环的元素，除一个元素是例外，其余都有一个右拟逆元素.

4. 陣环 令$\mathfrak{R}$是一个任意环，今来定义元素在$\mathfrak{R}$里的$n\times n$**陣**环$\mathfrak{R}_n$. $\mathfrak{R}_n$的元素是n行n列的陣

$$(a)=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}, \tag{4}$$

它的元素(也叫做系数或坐标) a_{ij} 属于基环 $\mathfrak{R}$. (a) 的第 i 行与第 j 列相交处的元素 a_{ij} 叫做 (a) 的 (i, j) 元素. 两个陣 (a) 与 (b) 作为相等,必須而且只須对于所有 i, j 都有 $a_{ij}=b_{ij}$; 而集合 $\mathfrak{R}_n$ 是元素属于 $\mathfrak{R}$ 的陣的全部.

陣的加法由公式

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2n}+b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1}+b_{n1} & a_{n2}+b_{n2} & \cdots & a_{nn}+b_{nn} \end{bmatrix}$$

来定义. 故求陣的和即是把在相同位置的元素 a_{ij} 与 b_{ij} 相加. 我們容易驗証: $\mathfrak{R}_n$ 及这样加法合成組成一个交换羣. 零陣是所有元素都等于 0 的陣, 而 (a) 的負陣是以 $-a_{ij}$ 作为 (i, j) 元素的陣, 亦即在第 i 行与第 j 列的交点处的元素为 $-a_{ij}$. 陣的乘法定义为

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} \sum a_{1k}b_{k1} & \sum a_{1k}b_{k2} & \cdots & \sum a_{1k}b_{kn} \\ \sum a_{2k}b_{k1} & \sum a_{2k}b_{k2} & \cdots & \sum a_{2k}b_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ \sum a_{nk}b_{k1} & \sum a_{nk}b_{k2} & \cdots & \sum a_{nk}b_{kn} \end{bmatrix}.$$

故积 $(p)=(a)(b)$ 的 (i, j) 元素为

$$p_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots+a_{in}b_{nj}.$$

例如,元素取在整数环 I 上,則在陣环 I_3 里有

$$\begin{bmatrix} 1 & -2 & 3 \\ 0 & 1 & -1 \\ 2 & 5 & -2 \end{bmatrix}\begin{bmatrix} 0 & 3 & 4 \\ 2 & 5 & 1 \\ -1 & -6 & 2 \end{bmatrix}=\begin{bmatrix} -7 & -25 & 8 \\ 3 & 11 & -1 \\ 12 & 43 & 9 \end{bmatrix}.$$

陣的乘法是可結合的．这因为，由乘法法則指出，积 $(a)[(b)(c)]$ 的 (i, j) 元素是 $\sum\limits_{k,l} a_{ik}(b_{kl}c_{lj})$，而 $[(a)(b)](c)$ 的 (i, j) 元素是 $\sum\limits_{k,l}(a_{ik}b_{kl})c_{lj}$．由于乘法在 $\mathfrak{R}$ 里适合結合律，故这两个元素相等．于是，

$$(a)[(b)(c)] = [(a)(b)](c).$$

分配律也是成立的．这因为 $(a)[(b)+(c)]$ 的 (i, j) 元素是 $\sum\limits_k a_{ik}(b_{kj}+c_{kj})$，而 $(a)(b)+(a)(c)$ 的 (i, j) 元素是 $\sum\limits_k a_{ik}b_{kj}+\sum\limits_k a_{ik}c_{kj}$．由于 $\mathfrak{R}$ 里元素适合分配律，故这两个元素相等．同理可証另一个分配律．

故 $\mathfrak{R}_n$ 是一个环．必須指出，$\mathfrak{R}$ 即使是交換环，在 $n>1$ 时，$\mathfrak{R}_n$ 不一定可交換（参看习題 25 的第 3 題）．如果 $n>1$，$\mathfrak{R}_n$ 还含有 $\neq 0$ 的零因子．

习　題　25

1. 計算

$$\begin{bmatrix} 1 & -2 & 3 \\ -2 & 1 & 3 \\ 0 & 1 & -1 \end{bmatrix}\begin{bmatrix} 3 & -5 & 6 \\ 7 & 2 & 1 \\ -1 & 1 & 2 \end{bmatrix}.$$

2. 用例来驗証 I_2 为非交換的，且含有 $\neq 0$ 的零因子．

3. 如果 $\mathfrak{R}\neq 0$，而 $n>1$，求証：$\mathfrak{R}_n$ 有 $\neq 0$ 的零因子．如果 $\mathfrak{R}$ 含有元素 a, b，使 $ab\neq 0$，$n>1$，求証：$\mathfrak{R}_n$ 为非交換的．

如果 $\mathfrak{R}$ 有一个恆等元素 1，显然元素

$$1=\begin{bmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix} \tag{5}$$

是环 $\mathfrak{R}_n$ 里的恆等元素．今設 $\mathfrak{R}$ 是交換环，我們来决定 $\mathfrak{R}_n$ 的单位元素乘法羣．为着这目的，需用陣的行列式．这里假定讀者已具

有任意阶行列式論的初等知識. 在初等代数或几何的教本里，关于行列式的通常处理对于元素在任一个交换环里的陣的行列式都适用.

这里先說陣的行列式的定义. 設陣 (a) 如 (4) 所示，則它的行列式 $\det(a)$ 是

$$\sum_{P} \pm a_{1i_1}a_{2i_2}\cdots a_{ni_n}, \tag{6}$$

这里是对于 $(1, 2, \cdots, n)$ 的所有置换 $(i_1, i_2, \cdots, i_n)$ 求和，而符号 + 或 − 則按置换是偶的或是奇的而定. (4) 里元素 a_{ij} 的余因子是从 (a) 里划去第 i 行及第 j 列后所得的 $n-1$ 阶行列式与 $(-1)^{i+j}$ 的积. 我們熟知，任一行(列)上各元素与它的余因子的积之和等于 $\det(a)$. 故若以 A_{ij} 表 a_{ij} 的余因子，則

$$\begin{aligned} &a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in} = \det(a), \\ &a_{1i}A_{1i} + a_{2i}A_{2i} + \cdots + a_{ni}A_{ni} = \det(a). \end{aligned} \tag{7}$$

我們还知道，任一行(列)上各元素与另一行(列)上对应元素的余因子的积之和等于 0:

$$\begin{aligned} &a_{i1}A_{j1} + a_{i2}A_{j2} + \cdots + a_{in}A_{jn} = 0, \quad i \neq j; \\ &a_{1i}A_{1j} + a_{2i}A_{2j} + \cdots + a_{ni}A_{nj} = 0, \quad i \neq j. \end{aligned} \tag{8}$$

这些关系引导我們来定义陣 (a) 的伴随陣 $\operatorname{adj}(a)$. (a) 的伴随陣是一个陣，它的 (i, j) 元素 $\alpha_{ij} = A_{ji}$. 应用这定义可見，法則 (7) 及 (8) 与陣方程

$$(a)\operatorname{adj}(a) = \begin{bmatrix} \det(a) & & & 0 \\ & \det(a) & & \\ & & \ddots & \\ 0 & & & \det(a) \end{bmatrix} = [\operatorname{adj}(a)](a) \tag{9}$$

等价. 故若 $\Delta = \det(a)$ 是 $\mathfrak{R}$ 里一个单位元素时，則以 $b_{ij} = \alpha_{ij}\Delta^{-1}$ 为 (i, j) 元素的陣 (b) 适合

$$(a)(b) = 1 = (b)(a), \tag{10}$$

这就証明了下面定理的充分性.

定理 1. 如果 $\mathfrak{R}$ 是帶恆等元素的一个交换环，陣 $(a) \in \mathfrak{R}_n$ 是一个單位元素必須而且只須它的行列式是 $\mathfrak{R}$ 里一个單位元素.

要証必要性，引用基本乘法法則

(11) $$\det[(a)(b)] = \det(a)\det(b).$$

于是，如果 $(a)(b) = 1$，則得 $\det(a)\det(b) = 1$. 故 $\det(a)$ 是一个单位元素.

这定理的一个可注意的特殊情形是

系 如果 $\mathfrak{R} = \mathfrak{F}$ 是一个域，則陣 $(a) \in \mathfrak{F}_n$ 是一个單位元素必須而且只須它的行列式不等于零.

习 題 26

1. 求陣

$$\begin{bmatrix} -1 & 2 & 4 \\ 3 & 2 & 0 \\ 5 & -1 & 2 \end{bmatrix}$$

的伴随陣.

2. 証明陣

$$\begin{bmatrix} 1 & 4 & 1 \\ 0 & 1 & -1 \\ -3 & -6 & -8 \end{bmatrix}$$

是 I_3 里一个单位元素，这里 I 是整数环. 并求这个陣的逆陣.

3. 如果 $\mathfrak{R}$ 是带恆等元素的交換环，而 $(a), (b) \in \mathfrak{R}_n$，求証: $(a)(b) = 1$ 可推得 $(b)(a) = 1$.

5. 四維数

設 C 是复数域，我們考究 C_2 里形状如

(12) $$\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \equiv \begin{bmatrix} \alpha_0 + \alpha_1\sqrt{-1} & \alpha_2 + \alpha_3\sqrt{-1} \\ -\alpha_2 + \alpha_3\sqrt{-1} & \alpha_0 - \alpha_1\sqrt{-1} \end{bmatrix}$$

(α_i 是实数)

的陣的集合 Q. 我們要証: Q 是 C_2 的加法羣的一个子羣，及 Q 对于乘法封閉. 前者是容易驗証的. 因为

$$\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}\begin{bmatrix} c & d \\ -\bar{d} & \bar{c} \end{bmatrix} = \begin{bmatrix} ac - b\bar{d} & ad + b\bar{c} \\ -\bar{b}c - \bar{a}\bar{d} & \bar{a}\bar{c} - \bar{b}d \end{bmatrix},$$

故积的形状为

$$\begin{bmatrix} u & v \\ -\bar{v} & \bar{u} \end{bmatrix},$$

这里，$u = ac - b\bar{d}$, $v = ad + b\bar{c}$. 故它属于 Q. 因为結合律、

加法交换律及分配律都从 C_2 轉移到子集合 Q，故 Q，+，· 显然是一个环．因此，Q，+，· 按下面的定义是环 C_2，+，· 的子环的一个例子．

定义 2. 設 $\mathfrak{B}$ 是环 $\mathfrak{A}$ 的一个子集合，它对于环的合成封閉，且 $\mathfrak{B}$，+，·（$\mathfrak{A}$ 的合成所导出的合成）是一个环，則 $\mathfrak{B}$，+，· 叫做 $\mathfrak{A}$，+，· 的一个子环．

由这里考究显見，如果一个子集合 $\mathfrak{B}$ 具有 $\mathfrak{B}$，+ 成一个羣，而 $\mathfrak{B}$ 对于乘法封閉时，則 $\mathfrak{B}$ 决定一个子羣．前一个条件也可說为：(1) 如果 $\mathfrak{B}$ 对于＋封閉，且在 $\mathfrak{B}$ 里含有 0 及每个元素的負元素，或 (2) 如果 $\mathfrak{B}$ 对于減法封閉．

今証 Q 是一个除环．首先我們知道，如果 (12) 的陣 $\neq 0$，則

$$\det\begin{bmatrix} \alpha_0+\alpha_1\sqrt{-1} & \alpha_2+\alpha_3\sqrt{-1} \\ -\alpha_2+\alpha_3\sqrt{-1} & \alpha_0-\alpha_1\sqrt{-1}\end{bmatrix}=\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2\neq 0.$$

故这个陣有一个逆陣；用前节方法得它的逆陣为

$$\begin{bmatrix} (\alpha_0-\alpha_1\sqrt{-1})\Delta^{-1} & -(\alpha_2+\alpha_3\sqrt{-1})\Delta^{-1} \\ (\alpha_2-\alpha_3\sqrt{-1})\Delta^{-1} & (\alpha_0+\alpha_1\sqrt{-1})\Delta^{-1}\end{bmatrix},$$

这里 $\Delta=\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2$．故逆陣属于 Q．于是，我們証得 Q 里任一个元素都有一个逆元素，它也属于 Q．故 Q 是一个除环．我們叫 Q 做（汉米頓 (Hamilton) 的）四維数环，而 Q 的元素叫做四維数．

环 Q 含有如

$$\alpha'=\begin{pmatrix}\alpha & 0\\ 0 & \alpha\end{pmatrix} \tag{13}$$

形的陣所构成的子环 R'．这种陣易知与 C_2 里每个陣可交換；因此也与每个四維数可交換．应該指出，陣

$$i=\begin{pmatrix}\sqrt{-1} & 0\\ 0 & -\sqrt{-1}\end{pmatrix},\quad j=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}, \tag{14}$$

$$k=\begin{pmatrix}0 & \sqrt{-1}\\ \sqrt{-1} & 0\end{pmatrix}$$

都是四維数．我們可驗証

$$\begin{bmatrix} \alpha_0+\alpha_1\sqrt{-1} & \alpha_2+\alpha_3\sqrt{-1} \\ -\alpha_2+\alpha_3\sqrt{-1} & \alpha_0-\alpha_1\sqrt{-1} \end{bmatrix} = \alpha_0'+\alpha_1'i+\alpha_2'j+\alpha_3'k.$$

故若 $\alpha_0'+\alpha_1'i+\alpha_2'j+\alpha_3'k=\beta_0'+\beta_1'i+\beta_2'j+\beta_3'k$，則

$$\begin{bmatrix} \alpha_0+\alpha_1\sqrt{-1} & \alpha_2+\alpha_3\sqrt{-1} \\ -\alpha_2+\alpha_3\sqrt{-1} & \alpha_0-\alpha_1\sqrt{-1} \end{bmatrix} = \begin{bmatrix} \beta_0+\beta_1\sqrt{-1} & \beta_2+\beta_3\sqrt{-1} \\ -\beta_2+\beta_3\sqrt{-1} & \beta_0-\beta_1\sqrt{-1} \end{bmatrix},$$

而有 $\alpha_i=\beta_i$ 及 $\alpha_i'=\beta_i'$．这指明，四維数用形状 $\alpha_0'+\alpha_1'i+\alpha_2'j+\alpha_3'k$ 表出是唯一的．因为

(15) $$(\alpha+\beta)'=\alpha'+\beta',\quad (\alpha\beta)'=\alpha'\beta',$$

故积

$$(\alpha_0'+\alpha_1'i+\alpha_2'j+\alpha_3'k)(\beta_0'+\beta_1'i+\beta_2'j+\beta_3'k)$$

可由 $\mathfrak{R}$ 里的加法与乘法及由乘法表

(16) $$i^2=j^2=k^2=-1',$$

$$ij=-ji=k,\quad jk=-kj=i,\quad ki=-ik=j$$

决定．这表恰好指出：Q 不是可交換的．最后要提醒的是，如果以 α 代替 α'，更一般地以 $\alpha_0+\alpha_1i+\alpha_2j+\alpha_3k$ 代替 $\alpha_0'+\alpha_1'i+\alpha_2'j+\alpha_3'k$，則記法就簡单了．我們在下面习題中就采取这样措施．

习　題　27

1. 計算 $(-1+2i-3j+k)(2-i+3j-2k)$．
2. 我們定义 $a=\alpha_0+\alpha_1i+\alpha_2j+\alpha_3k$ 的跡 $T(a)=2\alpha_0$，及距[1] $N(a)=\Delta=\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2$．驗証 a 适合二次方程 $x^2-T(a)x+N(a)=0$．
3. 求証：$N(ab)=N(a)N(b)$．
4. 設 α_i 是有理数，求証：四維数 $\alpha_0+\alpha_1i+\alpha_2j+\alpha_3k$ 的集合 Q_0 是 Q 的一个子除环，亦即 Q_0 是一个子环，并且是除环．
5. 如果 α_i 或者都是整数，或者都是奇整数的 1/2，驗証：四維数 $\alpha_0+\alpha_1i+\alpha_2j+\alpha_3k$ 的集合 I 是 Q 的一个子环．I 是否一个除环呢？

6. 由元素的集合生成的子环，心　由子环的定义显然可知，如

1) 距也有譯作模方——譯者注．

果一个环的若干子集合都决定子环，则它們的交也有这个性質．用更簡单的句子叙述它，我們說，由一个环的子环組成的任一个集合的交是一个子环． 如果 S 是环 $\mathfrak{A}$ 的任一个子集合，則含有 S 的各子环的交叫做由 S 生成的子环，記做 $[[S]]$． 显然，$[[S]]$ 可由下面的性質刻划出来：

(1)　$[[S]]$ 是一个子环，

(2)　$[[S]]\supseteq S$，

(3)　如果 $\mathfrak{B}$ 是含有 S 的任一个子环，則 $\mathfrak{B}\supseteq[[S]]$．

$[[S]]$ 的元素的形状是容易写出的，它是元素 $\sum\pm s_1s_2\cdots s_r$；換句話說，是 S 里元素 s_i 的有限积，及負的这样积之和． 这因为，这种和的集合是一个子环． 显然，它具有 $[[S]]$ 的性質 (2) 及 (3)．

設 S 是元素的一个集合，則与每个 $s\in S$ 可交換的元素 c 的全部 $C(S)$ 是一个子环． 如果 $S_1\supseteq S_2$，显然 $C(S_1)\subseteq C(S_2)$，并且 $C(C(S))\supseteq S$． 由这两个关系得出有趣的

$$C(C(C(S)))=C(S).$$

这因为，在 $C(C(S))\supseteq S$ 里以 $C(S)$ 代 S，就得出 $C(C(C(S)))\supseteq C(S)$． 另一方面，如果在这个关系的两端施以运算 C，則得 $C(C(C(S)))\subseteq C(S)$．合併这两个結果得 $C(C(C(S)))=C(S)$．

就 $[[S]]$ 的元素的形状来說，可知：如果元素 c 与 S 的各元素可交換，則也与 $[[S]]$ 的各元素可交換．故 $C(S)=C([[S]])$．

子环 $\mathfrak{C}=C(\mathfrak{A})$ 叫做环的心． 如果 $\mathfrak{A}$ 含有恆等元素 1，显然，$1\in\mathfrak{C}$．

习　　題 28

1．决定四維数环的心．

2．令

$$(\alpha)=\begin{bmatrix}\alpha_1 & & & 0\\ & \alpha_2 & & \\ & & \ddots & \\ 0 & & & \alpha_n\end{bmatrix}$$

里的 α_i 是不同的有理数，R_0 是有理数域，求証：陣环 R_{0n} 里的 $C(\alpha)$ 是对角陣的集合，亦即是与 (α) 形状相同的陣的集合．

3．求証：R_{0n} 的心是純量陣

$$\begin{bmatrix} \alpha & & & 0 \\ & \alpha & & \\ & & \ddots & \\ 0 & & & \alpha \end{bmatrix}$$

的集合。

4. 設 S 是 I_2 里如 $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ 形状的陣的集合，求 $C(S)$。

7. 理想，差环 令 $\mathfrak{B}$ 是 $\mathfrak{A}$ 的加法羣的一个子羣．因为加法是可交換的，故 $\mathfrak{B}$ 是一个不变子羣，并且

(17) $$(a+\mathfrak{B})+(c+\mathfrak{B})=(a+c)+\mathfrak{B},$$

这里加法是对于子集合定义它們的加法（就是說，$U+V$ 是元素 $u+v$ 的全部，$u\in U$, $v\in V$）．这样得来陪集的集合 $\bar{\mathfrak{A}}\equiv\mathfrak{A}/\mathfrak{B}$ 关于这个加法合成是一个交換羣．因此，就引起了下面的問題：对于 $\mathfrak{A}$ 里所有 a, a', c, c' 要使 $a\equiv a' \pmod{\mathfrak{B}}$, $c\equiv c' \pmod{\mathfrak{B}}$ 能推出 $ac\equiv a'c' \pmod{\mathfrak{B}}$，則 $\mathfrak{B}$ 应适合什么条件呢？設已选定 a 及 c，則 $a'=a+b_1$ 及 $c'=c+b_2$，这里 b_1 与 b_2 都属于 $\mathfrak{B}$．显然，b_1 与 b_2 的任一种选取各給出一个 $a'\equiv a \pmod{\mathfrak{B}}$ 及 $c'\equiv c \pmod{\mathfrak{B}}$．因此，我們的要求相当于

$$(a+b_1)(c+b_2)=ac+ab_2+b_1c+b_1b_2\equiv ac \pmod{\mathfrak{B}},$$

对于所有 $a, c\in\mathfrak{A}$ 与所有 $b_1, b_2\in\mathfrak{B}$ 都成立．于是，对于所有 a, $c\in\mathfrak{A}$ 与所有 $b_1, b_2\in\mathfrak{B}$，需要

(18) $$ab_2+b_1c+b_1b_2\in\mathfrak{B}.$$

取 $b_1=0$，得出：对于所有 $a\in\mathfrak{A}$ 与所有 $b\in\mathfrak{B}$，需要

(L) $$ab\in\mathfrak{B};$$

又取 $b_2=0$，得出：对于所有 $a\in\mathfrak{A}$ 与所有 $b\in\mathfrak{B}$，需要

(R) $$ba\in\mathfrak{B}.$$

反过来，如果 (L) 及 (R) 成立，則当 b_1 及 b_2 属于 $\mathfrak{B}$ 时，ab_2, b_1c 及 b_1b_2 都属于 $\mathfrak{B}$，故 (18) 也就成立．这就导致重要的定义：

定义 3. 設 $\mathfrak{B}$ 为环 $\mathfrak{A}$ 的一个子集合，如果 $\mathfrak{B}$, $+$ 是 $\mathfrak{A}$ 的加法羣的一个子羣，且 $\mathfrak{B}$ 具有封閉性 (L) 及 (R)，則 $\mathfrak{B}$ 叫做**理想**.

因为一个子集合 $\mathfrak{B}$ 决定一个子羣，必須而且只須每两个元素的差也含于这集合里；故 $\mathfrak{B}$ 是一个理想必須而且只須 (1)b_1,

$b_2 \in \mathfrak{B}$ 可推得 $b_1 - b_2 \in \mathfrak{B}$；(2) $b \in \mathfrak{B}$ 可推得 ab 及 ba 属于 $\mathfrak{B}$ 对于所有 $a \in \mathfrak{A}$ 都成立. 显然，理想对于乘法是封閉的，故一个理想决定 $\mathfrak{A}$ 的一个子环.

設 $\mathfrak{B}$ 是 $\mathfrak{A}$ 里一个理想，上面討論指出：如果 $a \equiv a' \pmod{\mathfrak{B}}$ 及 $c \equiv c' \pmod{\mathfrak{B}}$，則 $ac \equiv a'c' \pmod{\mathfrak{B}}$；換句話說，陪集 $a + \mathfrak{B}$ 里任一个元集与陪集 $c + \mathfrak{B}$ 里任一个元素的积是陪集 $ac + \mathfrak{B}$ 里一个元素. 故对于陪集可由公式

$$(a + \mathfrak{B})(c + \mathfrak{B}) = ac + \mathfrak{B} \tag{19}$$

定义一个(单値)乘法合成. 应該指出，这种乘法与在乘法半羣里定义的集合乘法不一致. 但因为我們沒有机会用到后者，故(19)里的記法不致发生什么混乱. 至此，我們可肯定：集合 $\mathfrak{A}/\mathfrak{B}$ 与加法(17)及乘法(19)組織成一个环. 这因为，关于加法的各个法則显然成立，所以只要驗証乘法的結合律及分配律即够了. 由于

$$[(a + \mathfrak{B})(c + \mathfrak{B})](d + \mathfrak{B}) = (ac + \mathfrak{B})(d + \mathfrak{B}) = (ac)d + \mathfrak{B},$$

$$(a + \mathfrak{B})[(c + \mathfrak{B})(d + \mathfrak{B})] = (a + \mathfrak{B})(cd + \mathfrak{B}) = a(cd) + \mathfrak{B}$$

及

$$\begin{aligned}(a + \mathfrak{B})[(c + \mathfrak{B}) + (d + \mathfrak{B})] &= (a + \mathfrak{B})(c + d + \mathfrak{B}) \\ &= a(c + d) + \mathfrak{B},\end{aligned}$$

$$\begin{aligned}(a + \mathfrak{B})(c + \mathfrak{B}) + (a + \mathfrak{B})(d + \mathfrak{B}) &= (ac + \mathfrak{B}) + (ad + \mathfrak{B}) \\ &= (ac + ad) + \mathfrak{B},\end{aligned}$$

还有一个分配律也可用类似的計算来完成，就可見乘法結合律及分配律都是成立的. $\mathfrak{A}/\mathfrak{B}$ 与上面定义的合成所决定的环叫做 $\mathfrak{A}$ **关于理想 $\mathfrak{B}$ 的差(商，剩余类)环.**

环的某些初等性質会轉移到差环中去. 譬如，設 $\mathfrak{A}$ 是交換环，則 $\mathfrak{A}/\mathfrak{B}$ 也是交換环，这可由定义立見. 仿此，設 $\mathfrak{A}$ 有恆等元素 1，則 $\bar{1} = 1 + \mathfrak{B}$ 是 $\mathfrak{A}/\mathfrak{B}$ 里的恆等元素. 但另一方面，我們在下一节中看到 $\mathfrak{A}$ 是一个整区，而差环可能不是整区.

习 题 29

1. 如果 n 是整数，求証：na 形的元素的集合 $n\mathfrak{A}$ 是一个理想.
2. 求証：在任一个环 $\mathfrak{A}$ 里，使 $na = 0$ 的元素 a 的集合 $\mathfrak{N}$ 是一个理想.

8. 关于整数环的理想及差环 設 m 是任一个整数，m 的倍数的集合 (m)[1] 是整数环 I 里的一个理想. 这因为，我們知道，(m) 是加法羣 I 的一个子羣，并且 m 的倍数的倍数显然是 m 的倍数. 又因为集合 (m) 是 I 的唯一子羣，所以也是环 I 里唯一的理想. 因为 $(m) = (-m)$，故只須就 $m = 0$ 及 $m > 0$ 来討論. 設 $m = 0$，则 $(m) = 0$；于是，$I/(m) = I$. 今假定 $m > 0$，则 $I/(m)$ 有 m 个元素

$\bar{0} = 0 + (m)$，$\bar{1} = 1 + (m)$，$\cdots$，$\overline{(m-1)} = m - 1 + (m)$，

而元素 $\bar{1} = 1 + (m)$ 是 $I/(m)$ 的恆等元素.

先設 m 为合数，令 $m = m_1m_2$，这里 $m_i > 1$，则 m 不能除尽 m_i，而且 $\bar{m}_i \neq 0$. 但 $\bar{m}_1\bar{m}_2 = \overline{m_1m_2} = \bar{m} = 0$，故知 $I/(m)$ 不是一个整区.

次設 $m = p$ 是不可約数(或素数)，亦即 p 不能写成大于 1 的整数的积. 此时可証：$I/(p)$ 是一个域. 首先，$I/(p)$ 有一个恆等元素. 次令 $\bar{a} \neq 0$，则 a 不能被 p 除尽，故若 $d = (a, p)$，则 $d \neq p$；因为 p 是素数，这样就只有 $d = 1$. 故有整数 b 及 q 存在，使 $ab + pq = 1$. 于是，$\bar{a}\bar{b} = \overline{ab} = \bar{1}$. 故在 $I/(p)$ 里，$\bar{a}$ 有逆元素 $\bar{b}$. 从上面討論得出有趣結論：对于任一个素数 p，必有包含 p 个元素的域存在.

如果弃去 m 是素数的假設，而企图决定 $I/(m)$ 里单位元素. 令 M 表单位元素的集合，并令 $\bar{a} \in M$. 則有 $\bar{b}$ 存在，使 $\bar{a}\bar{b} = \bar{1}$. 于是，$ab = 1 + mq$，而 $ab - mq = 1$. 由此推得 $(a, m) = 1$. 反过来，如果 $(a, m) = 1$，则存在有 b，q，使 $ab - mq = 1$. 故 $\bar{a}\bar{b} = 1$. 这指出了：$\bar{0}$，$\bar{1}$，$\bar{2}$，$\cdots$，$\overline{m-1}$ 里单位元素是适合条件 $(a, m) = 1$ 的各陪集 $\bar{a}$. 这就証明了下面的定理.

---

1) 关于这个集合的羣的記法是 $[m]$. ——著者注.

定理 2. $I/(m)$ 的單位元素的羣 M 的階數等于比 m 小而与 m 互素 $((a, m) = 1)$ 的正整數个數.

这个数記做 $\phi(m)$. 这样决定得的 m 的函数叫做欧拉 ϕ 函数(指示函数).

如果 $\mathfrak{G}$ 是 n 阶有限羣, 則对于每个 $a \in \mathfrak{G}$, $a^n = 1$. 应用这結果于 M, 可見: 如果 $(a, m) = 1$, 則 $(\bar{a})^{\phi(m)} = \bar{1}$. 这个方程与 $a^{\phi(m)} \equiv 1 \pmod m$ 等价. 故得下面定理.

定理 3. (欧拉-斐瑪 (Euler-Fermat) 定理) 設整數 a 与正整數 m 互素, 則

$$a^{\phi(m)} \equiv 1 \pmod m.$$

設 $m = p$, 則 $I/(p)$ 是 p 个元素的域, 此时单位元素的羣含有 $p - 1$ 个元素, 故得:

系. 如果 p 是素數, 而 $a \not\equiv 0 \pmod p$, 則 $a^{p-1} \equiv 1 \pmod p$.

这个結果可用稍微不同的形状述出, 即 $a^p \equiv a \pmod p$. 因为, 如果 a 可被 p 除尽, 則这結果是显然的; 故乜对于所有 a 成立. 另一方面, 如果 $a^p \equiv a \pmod p$ 而且 $a \not\equiv 0 \pmod p$, 則 $a^{p-1} \equiv 1 \pmod p$. 故两种說法是等价的.

习 題 30

1. 如果 D 是含有 q 个元素的有限除环, 求証: 对于每个 $a \in D$, $a^q = a$.

9. 环的同态

定义 4. 設 η 是环 $\mathfrak{A}$ 到环 $\mathfrak{A}'$ 内的一个映照, 如果

$$(a + b)\eta = a\eta + b\eta, \quad (ab)\eta = (a\eta)(b\eta),$$

則 η 叫做一个同态.

故环的同态是乜的加法羣的一个同态, 并且"保持"乘法的. 如果 η 是 1—1 映照, 則叫做同构. 如果 $\mathfrak{A}$ 到 $\mathfrak{A}'$ 上存在一个同构, 就說这两个环是同构的 $(\mathfrak{A} \cong \mathfrak{A}')$. 与羣的情形相似, 易知: 两个同态的积是一个同态. 又設 η 是 $\mathfrak{A}$ 到 $\mathfrak{A}'$ 上一个同构, 則逆映照 η^{-1} 是 $\mathfrak{A}'$ 到 $\mathfrak{A}$ 上的一个同构. 故在环方面, 同构关系是一种等价关系. 一个环到乜自身上的同构叫做自同构. 这些概念于下面习

題中得到說明.

习 题 31

1. 驗証:对应 $\alpha+\beta\sqrt{-1}\to\begin{pmatrix}\alpha & \beta\\ -\beta & \alpha\end{pmatrix}$ 是复数域 C 到 R_2 内的一个同构.
2. 驗証:对应 $a=\alpha+\beta\sqrt{-1}\to\bar{a}=\alpha-\beta\sqrt{-1}$ 是 C 里一个自同构.
3. 驗証:对应 $\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}\to\alpha$ 是对角陣环到它的系数环 $\mathfrak{R}$ 内的一个同态.
4. 驗証:对应

$$\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k\to\begin{bmatrix}\alpha_0 & \alpha_1 & \alpha_2 & \alpha_3\\ -\alpha_1 & \alpha_0 & -\alpha_3 & \alpha_2\\ -\alpha_2 & \alpha_3 & \alpha_0 & -\alpha_1\\ -\alpha_3 & -\alpha_2 & \alpha_1 & \alpha_0\end{bmatrix}$$

是 Q 到 R_4 内的一个同构.

环同态的理論与羣同态的理論是平行的，而且一部分是由后者导出. 今从叙述下面的基本結果开始.

定理 4. 如果 η 是 $\mathfrak{A}$ 到 $\mathfrak{A}'$ 内的一个同态,則像集合 $\mathfrak{A}\eta$ 是 $\mathfrak{A}'$ 的一个子环.

証 因为 η 是 $\mathfrak{A}$ 的加法羣的一个同态，故 $\mathfrak{A}\eta$ 是 $\mathfrak{A}'$ 的加法羣的一个子羣. 因为 $(a\eta)(b\eta)=(ab)\eta$，故 $\mathfrak{A}\eta$ 对于乘法封閉. 所以它是一个子环.

設环 $\mathfrak{A}$ 有恆等元素 1，則易知 $1'=1\eta$ 是 $\mathfrak{A}\eta$ 的恆等元素.又設 u 是单位元素，以 v 为它的逆元素，則 $u'=u\eta$ 是 $\mathfrak{A}\eta$ 里一个单位元素,以 $v'=v\eta$ 为它的逆元素. 当然我們会遇到 $1\eta=0$ 的情形，此时 $\mathfrak{A}\eta=0$. 在特殊情形，如果 $\mathfrak{A}$ 是一个除环，則或者 $\mathfrak{A}\eta=0$，或者 $\mathfrak{A}\eta$ 也是一个除环. 这因为，如果 $\mathfrak{A}\eta\neq 0$，則这个环不只含一个元素,而且每个非零元素都是一个单位元素.

我們也照羣的情形,把逆象 $\eta^{-1}(0)$ 叫做同态 η 的核. 同态 η 是一个同构必須而且只須它的核是 0.

定理 5. 环 $\mathfrak{A}$ 的一个同态的核是 $\mathfrak{A}$ 里一个理想.

証 令 $\mathfrak{K}=\eta^{-1}(0)$. 我們知道，$\mathfrak{K}$ 是 $\mathfrak{A}$ 的加法羣的一个子羣. 今令 $b\in\mathfrak{K}$，并令 a 是 $\mathfrak{A}$ 里任意元素，則 $(ab)\eta=(a\eta)(b\eta)=(a\eta)0=0$. 故 $ab\in\mathfrak{K}$. 同理，$ba\in\mathfrak{K}$，而証明完成.

次令$\mathfrak{B}$是环里任一个理想，并令$\bar{\mathfrak{A}}$表示差环$\mathfrak{A}/\mathfrak{B}$. 我們知道，自然映照$\nu$是$\mathfrak{A}$的加法羣到$\bar{\mathfrak{A}}$的加法羣上的一个同态. 还有

$$(a_1a_2)\nu = a_1a_2 + \mathfrak{B} = (a_1 + \mathfrak{B})(a_2 + \mathfrak{B}) = (a_1\nu)(a_2\nu).$$

故ν是环$\mathfrak{A}$到环$\bar{\mathfrak{A}}$上的一个同态.

今設η是环$\mathfrak{A}$到环$\mathfrak{A}'$內的一个同态，同态核是$\mathfrak{K}$. 令$\mathfrak{B}$是$\mathfrak{A}$的一个理想含于$\mathfrak{K}$里，則易知，$a + \mathfrak{B} \to a\eta$ 定义$\bar{\mathfrak{A}} = \mathfrak{A}/\mathfrak{B}$的加法羣到$\mathfrak{A}'$的加法羣內一个同态$\bar{\eta}$. 因为

$$\begin{aligned}[(a_1 + \mathfrak{B})(a_2 + \mathfrak{B})]\bar{\eta} &= (a_1a_2 + \mathfrak{B})\bar{\eta} \\ &= (a_1a_2)\eta = (a_1\eta)(a_2\eta) = [(a_1 + \mathfrak{B})\bar{\eta}][(a_2 + \mathfrak{B})\bar{\eta}],\end{aligned}$$

故$\bar{\eta}$是一个环同态. 显然，$\eta = \nu\bar{\eta}$. 我們已知，$\bar{\eta}$是1—1的必須而且只須$\mathfrak{B} = \mathfrak{K}$. 故若取$\mathfrak{B} = \mathfrak{K}$，則得$\eta$的一个因子分解如$\nu\bar{\eta}$，这里$\nu$是$\mathfrak{A}$到$\bar{\mathfrak{A}} = \mathfrak{A}/\mathfrak{K}$上的自然同态，而$\bar{\eta}$是$\bar{\mathfrak{A}}$到$\mathfrak{A}'$內的导出同构. 綜合这些結果得下面的重要定理:

定理 6. 令η是环$\mathfrak{A}$到环$\mathfrak{A}'$內的一个同态，核为$\mathfrak{K}$；并令$\mathfrak{B}$是$\mathfrak{A}$的一个理想含于$\mathfrak{K}$里. 則对应$\bar{\eta}: a + \mathfrak{B} \to a\eta$是$\bar{\mathfrak{A}} = \mathfrak{A}/\mathfrak{B}$到$\mathfrak{A}'$內一个同态，并且$\eta = \nu\bar{\eta}$，这里$\nu$是$\mathfrak{A}$到$\bar{\mathfrak{A}} = \mathfrak{A}/\mathfrak{B}$上的自然映照. 导出同态$\bar{\eta}$是一个同構必須而且只須$\mathfrak{B} = \mathfrak{K}$.

設$\mathfrak{A}' = \mathfrak{A}\eta$，而$\mathfrak{B} = \mathfrak{K}$，則$\bar{\eta}$是$\bar{\mathfrak{A}}$到$\mathfrak{A}'$上的一个同构. 这結果与上面結果合併，得:

环的同态的基本定理 $\mathfrak{A}$关于任一个理想$\mathfrak{B}$的差环$\mathfrak{A}/\mathfrak{B}$，是$\mathfrak{A}$的一个同态像. 反过來，$\mathfrak{A}$的任一个同态像必与一个差环同構的. 事实上，与$\mathfrak{A}$关于同态核的差环是同構的.

如果环$\mathfrak{A}$里唯一的理想只是$\mathfrak{A}$及0（这些当然是任一个环的理想），这环叫做单純环. 設$\mathfrak{A}$是单純环，則由基本定理易知：$\mathfrak{A}$的同态象或者是0，或者与$\mathfrak{A}$是同构的.

次設环$\mathfrak{A}$有恆等元素e，且是由e生成的. 我們今来决定$\mathfrak{A}$的結构，作为上面結果的另一应用. 試考究整数环I及I到$\mathfrak{A}$內的映照$n \to ne$. 因为

$$(n + m)e = ne + me,$$
$$(nm)e = (nm)e^2 = (ne)(me),$$

故这对应是一个同态. 象集合 Ie 是 $\mathfrak{A}$ 的一个子环, 含有 $1e = e$, 故 $Ie = \mathfrak{A}$, 并且 $\mathfrak{A}$ 是 I 的一个同态象. 于是, $\mathfrak{A} \cong I/(m)$, 这里 $m \geqslant 0$. 因此, 或者 $\mathfrak{A}$ 是无限的, 而与整数环是同构的, 或者 $\mathfrak{A}$ 只有有限 m 个元素, 而与有限环 $I/(m)$ 是同构的.

习 题 32

1. 令 $m = rs \in I$. 驗証: $(r)/(m)$ 是 $I/(m)$ 里一个理想, 并証:

$$[I/(m)]/[(r)/(m)] \cong I/(r).$$

2. 試在形如 $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ 的陣所构成的 I_2 的子环里, 决定理想; 并由此决定同态象.

3. 如果 $a \to \bar{a}$ 是 $\mathfrak{R}$ 到 $\bar{\mathfrak{R}}$ 内的一个同态, 求証: $(a_{ij}) \to (\bar{a}_{ij})$ 是 $\mathfrak{R}_n$ 到 $\bar{\mathfrak{R}}_n$ 内的一个同态.

4. 令 η 是环 $\mathfrak{A}$ 到它自身内的一个同态, 驗証: 被 η 所固定, 亦即使 $a\eta = a$ 的 $\mathfrak{A}$ 里元素成一个子环. 如果 $\mathfrak{A}$ 是一个除环, 并且 $\mathfrak{A}\eta \neq 0$, 则固定元素的集合构成一个子除环.

5. 求証: I 到它自身内仅有的同态是恒等映照及把每个元素映到 0 的映照. 求就有理数域証明同一結果.

6. 令 $\mathfrak{B}$ 是一个集合, 并令 η 是 $\mathfrak{B}$ 到环 $\mathfrak{A}$ 上的一个 1—1 映照. 求証: 合成

$$a + b \equiv (a\eta + b\eta)\eta^{-1}, \quad ab \equiv ((a\eta)(b\eta))\eta^{-1}$$

把 $\mathfrak{B}$ 变到与 $\mathfrak{A}$ 同构的环. 应用这結果証明: 任一个环也是关于下面合成的一个环:

$$a \oplus b = a + b - 1, \quad a \cdot b = a + b - ab.$$

10. 反同构 設 a 是四維数 $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, 则四維数

$$\bar{a} = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$$

叫做 a 的共軛数. 如果参考 §5, 则可見, $a \neq 0$ 的逆元素 a^{-1} 可借公式 $a^{-1} = \bar{a}N(a)^{-1} = N(a)^{-1}\bar{a}$ 由共軛数表出. 今考究对应 $a \to \bar{a}$ 的性質. 这映照显然是 Q 到它自身上的 1—1 映照, 而且显然有

$$\overline{a + b} = \bar{a} + \bar{b}; \tag{20}$$

我們还可驗証

$$\begin{aligned}\overline{ab} = {} & (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3) \\ & - (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2)i - (\alpha_0\beta_2 + \alpha_2\beta_0 \\ & + \alpha_3\beta_1 - \alpha_1\beta_3)j - (\alpha_0\beta_3 + \alpha_3\beta_0 + \alpha_1\beta_2 - \alpha_2\beta_1)k,\end{aligned}$$

及

$$\begin{aligned}\bar{b}\bar{a} = {} & (\beta_0\alpha_0 - \beta_1\alpha_1 - \beta_2\alpha_2 - \beta_3\alpha_3) \\ & + (-\beta_0\alpha_1 - \beta_1\alpha_0 + \beta_2\alpha_3 - \beta_3\alpha_2)i + (-\beta_0\alpha_2 - \beta_2\alpha_0\end{aligned}$$

$+ \beta_3\alpha_1 - \beta_1\alpha_3)i + (-\beta_0\alpha_3 - \beta_3\alpha_0 + \beta_1\alpha_2 - \beta_2\alpha_1)k.$

故

(21) $$\overline{ab} = \bar{b}\bar{a}.$$

如果环 $\mathfrak{A}$ 到环 $\bar{\mathfrak{A}}$ 上的一个映照是 1—1 的，且适合 (20) 及 (21)，这映照叫做**反同构**. 如果 $\bar{\mathfrak{A}}$ 是可交换的，则可以 $\bar{a}\bar{b}$ 代 (21) 里的 $\bar{b}\bar{a}$，并且此时 $a \to \bar{a}$ 也是 $\mathfrak{A}$ 到 $\bar{\mathfrak{A}}$ 上的一个同构. 反过来，交换环間任一个同构可看作一个反同构. 特别是，如果 $\mathfrak{A}$ 是可交换的，则恆等映照是 $\mathfrak{A}$ 到它自身上一个反同构. 另一方面，由四維数的例子說明：也存在有非交换环，它对自身具有成反同构的对称性質. 現在再給出这种类型的另一个重要例子，即陣环 $\mathfrak{R}_n$，这里 $\mathfrak{R}$ 是任一个交换环.

为达到这目的，我們定义陣 (a) 的**轉置陣** $(a)'$ 是一个陣，它以 a_{ji} 做 (i, j) 元素，亦即 $(a)'$ 可由 (a) 的元素对于主对角綫作反射而得. 例如，設

$$(a) = \begin{pmatrix} 1 & 2 & -3 \\ 2 & -1 & 4 \\ 5 & -1 & 6 \end{pmatrix},$$

则

$$(a)' = \begin{pmatrix} 1 & 2 & 5 \\ 2 & -1 & -1 \\ -3 & 4 & 6 \end{pmatrix}.$$

通常如果 $(a) = (a_{ij})$, $(b) = (b_{ij})$，则 $(a) + (b) = (a_{ij} + b_{ij})$，而 $[(a) + (b)]'$ 的 (i, j) 元素是 $a_{ji} + b_{ji}$. 故 $[(a) + (b)]' = (a)' + (b)'$. 再則 $(p) = (a)(b)$ 的 (i, j) 元素是 $p_{ij} = \sum_k a_{ik}b_{kj}$，故 $(p)'$ 的 (i, j) 元素是 $p_{ji} = \sum_k a_{jk}b_{ki}$. 另一方面，$(b)'(a)'$ 的 (i, j) 元素是 $\sum_k b_{ki}a_{jk}$. 因为假定 $\mathfrak{R}$ 是可交换的，故得

$$[(a)(b)]' = (b)'(a)'.$$

于是 $(a) \to (a)'$ 显然是 1—1 的，并且是 $\mathfrak{R}$ 到它自身上的一个反同构.

对于任一个給定的环 $\mathfrak{A}, +, \cdot$，我們可作出一个反同构环．要达到这目的，我們使用原来的集合 $\mathfrak{A}$ 及給定的加法，但引入一个新的乘法 $\times$，定义为

$$a \times b = ba.$$

因

$$(a \times b) \times c = (ba) \times c = c(ba),$$
$$a \times (b \times c) = (b \times c)a = (cb)a,$$

及

$$a \times (b + c) = (b + c)a = ba + ca = a \times b + a \times c,$$
$$(b + c) \times a = a(b + c) = ab + ac = b \times a + c \times a,$$

故得一个环．易知恆等映照是 $\mathfrak{A}, +, \cdot$ 到 $\mathfrak{A}, +, \times$ 上的一个反同构．

习　　題　33

1．驗証：如 $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ 形的陣的集合，当 a 及 b 都 $\in I$ 时，是 I_2 的一个子环．它有一个左恆等元素，但无右恆等元素．于是，証明：这个环不与它自身成反同构．

2．对于半羣定义反同构．求証：任一个羣与它自身成反同构．

3．一个环到它自身上的一个反同构叫做反自同构．求証：一个环的自同构及反自同构构成一个变换羣．驗証：在这个羣里自同构构成指标为 1 或 2 的一个不变子羣．

4．如果 $a \to \bar{a}$ 是 $\mathfrak{R}$ 到 $\mathfrak{R}$ 上的一个反自同构，驗証：映照 $(a) \to (\bar{a})'$ 是 $\mathfrak{R}_n$ 到 $\mathfrak{R}_n$ 上的一个反同构，这里 $(\bar{a})'$ 的 (i, j) 元素是 $\bar{a}_{ji}$．

5．試定义反同态．說出并且証明对于反同态的“基本定理”．

6．求証华罗庚定理：令 S 是环 $\mathfrak{A}$ 到环 $\mathfrak{B}$ 內的一个映照，使 $(a + b)^S = a^S + b^S$，并且对于每两个元素 a, b，或者 $(ab)^S = a^S b^S$，或者 $(ab)^S = b^S a^S$．則 S 或者是一个同态，或者是一个反同态．

11．环的加法羣的結构．环的特征数　設 $\mathfrak{A}, +$ 是任一个交換羣，对于 $\mathfrak{A}$ 里所有 a, b 可定义乘法为 $ab = 0$，則得一个环．这合成显然是可結合的，并且关于加法是可分配的．这类型的环叫做零环．这样环的存在，說明了我們对于环的加法羣的結构一般沒有什么好說的．但我們将要指出：如果对于环的乘法半羣予以簡单的限制，会給加法羣带来強烈的限制．

例如，設 $\mathfrak{A}$ 有一个恆等元素 1，并設 1 在 $\mathfrak{A}, +$ 里的阶是有限的，等于 m．如果 a 是 $\mathfrak{A}$ 的任一个元素，則

$$ma = m(1a) = (m1)a = 0a = 0.$$

于是，每个元素有有限阶数，是 m 的一个因子。

如果 $\mathfrak{A}$，+ 的元素的阶有一个最大数 $m(>0)$ 存在，则 m 叫做 $\mathfrak{A}$ 的特征数。如果这样最大数不存在，则説 $\mathfrak{A}$ 有特征数 0（或无限大）[1]。因此，我們知道，如果 $\mathfrak{A}$ 有一个恆等元素 1，它的特征数 $m>0$，或 0，是按 1 在 $\mathfrak{A}$，+ 里的阶数是 m 或无限大而定。

这結果可以拓广。譬如，設 d 是 $\mathfrak{A}$ 的一个元素，有有限阶 m，并且 d 不是左零因子。如果 a 是 $\mathfrak{A}$ 的任一个元素，则

$$0 = (md)a = d(ma).$$

故 $ma = 0$。于是，$\mathfrak{A}$ 的特征数仍然是 m。对于不是右零因子，类似的結果当然也成立。

特别是，我們知道：如果 $\mathfrak{A}$ 是一个整区，則它的特征数或者是 0，或者是 $m>0$，并且每个非零元素的阶数都是 m。今来証明：在这种情形下，m 是素数。这因为，如果令 $m = m_1m_2$，这里 $m_i>1$，則当 $a \neq 0$ 时，

$$ma^2 = m_1m_2a^2 = (m_1a)(m_2a).$$

因为 $m_1a \neq 0$ 及 $m_2a \neq 0$，这就与定义矛盾。故得下面的定理：

定理 7. 如果 $\mathfrak{A}$ 是特征數 0 的一个整区，則 $\mathfrak{A}$ 的所有非零元素有无限階。如果 $\mathfrak{A}$ 的特征數 $m>0$，則 m 是一个素數，并且 $\mathfrak{A}$ 的所有非零元素的階數是 m。

习　题　34

1. 驗証：在定理 7 里用单純环代替整区也能成立。

12. 环的加法羣的子羣的代数．单側理想 本节討論某些重要合成，它可定义在环的加法羣的子羣的集合里。其中有两种合成：交及由子羣的集合生成的羣，已經对于任意羣討論过。現在我們从交換羣着手；故所有子羣都是不变的。所以，如果 $\mathfrak{A}$ 及 $\mathfrak{B}$ 是

1）"特征数无限大"一术語，就前面观点来説是較适宜的。但由另一个观点（参看第 3 章的 §8）来説，"特征数 0"也是适宜的。由于后者似覚最为通用，所以这里就这样沿用。——著者注。

子羣，則由 $\mathfrak{A}$ 及 $\mathfrak{B}$ 生成的子羣 $[\mathfrak{A}\cup\mathfrak{B}]$ 与和 $a+b$ 的集合 $\mathfrak{A}+\mathfrak{B}$ 重合，这里 $a\in\mathfrak{A}$, $b\in\mathfrak{B}$. 更一般地說，如果 $\{\mathfrak{A}_\alpha\}$ 是加法羣的子羣的一个集合，則由 $\mathfrak{A}_\alpha$ 生成的羣 $[\cup\mathfrak{A}_\alpha]$ 是有限和

$$a_{\alpha_1}+a_{\alpha_2}+\cdots+a_{\alpha_k},\quad a_{\alpha_i}\in\mathfrak{A}_{\alpha_i}$$

的集合；这因为，如果我們用 $\sum\mathfrak{A}_\alpha$ 来表示这些和的全部，可驗証它是加法羣的一个子羣. 再則 $\sum\mathfrak{A}_\alpha$ 包含所有 $\mathfrak{A}_\alpha$，并且被包含在具有这种性質的任一个子羣里. 故 $\sum\mathfrak{A}_\alpha$ 具有 $[\cup\mathfrak{A}_\alpha]$ 的各特性.

今引入关于加法羣的子羣的第三种合成. 設 $\mathfrak{A}$ 及 $\mathfrak{B}$ 是子羣，我們定义积 $\mathfrak{A}\mathfrak{B}$ 为由所有积 ab 生成的子羣，这里 $a\in\mathfrak{A}$, $b\in\mathfrak{B}$. 必須指出，这定义与关于陪集的乘法的定义不同. 因为关于子羣 $\mathfrak{B}$ 的各陪集里不等于 $\mathfrak{B}$ 的陪集不是子羣，故乘法記法虽作两用，仍不致发生任何实际上疑惑. 我們要知道，$\mathfrak{A}\mathfrak{B}$ 与有限和

$$a_1b_1+a_2b_2+\cdots+a_kb_k,\quad a_i\in\mathfrak{A},\quad b_i\in\mathfrak{B}$$

的集合 $\mathfrak{P}$ 相重合. 这因为，$\mathfrak{P}$ 显然包含所有积 ab，并且被包含于任一个能包含所有这些积的子羣里. 同时，$\mathfrak{P}$ 显然对于加法封閉，且含有 0. 最后，

$$-(a_1b_1+\cdots+a_kb_k)=(-a)b_1+\cdots+(-a_k)b_k\in\mathfrak{P}.$$

故 $\mathfrak{P}$ 是一个子羣. 由 $\mathfrak{P}$ 的这些性質自然可推得 $\mathfrak{P}=\mathfrak{A}\mathfrak{B}$.

由于子羣 $(\mathfrak{A}\mathfrak{B})\mathfrak{C}$ 及 $\mathfrak{A}(\mathfrak{B}\mathfrak{C})$ 是如 $\sum a_ib_ic_i$ 形的有限和的全部，这里 $a_i\in\mathfrak{A}$, $b_i\in\mathfrak{B}$, $c_i\in\mathfrak{C}$；故易証：結合律 $(\mathfrak{A}\mathfrak{B})\mathfrak{C}=\mathfrak{A}(\mathfrak{B}\mathfrak{C})$ 成立. 分配律

$$\mathfrak{A}(\mathfrak{B}+\mathfrak{C})=\mathfrak{A}\mathfrak{B}+\mathfrak{A}\mathfrak{C},\quad (\mathfrak{B}+\mathfrak{C})\mathfrak{A}=\mathfrak{B}\mathfrak{A}+\mathfrak{C}\mathfrak{A}$$

也是成立的. 我們可从 $\mathfrak{A}(\mathfrak{B}+\mathfrak{C})$ 是由所有积 $a(b+c)$ 生成的子羣这一事实来証第一个分配律，这里 $a\in\mathfrak{A}$, $b\in\mathfrak{B}$, $c\in\mathfrak{C}$. 因为

$$a(b+c)=ab+ac\in\mathfrak{A}\mathfrak{B}+\mathfrak{A}\mathfrak{C},$$

故 $\mathfrak{A}(\mathfrak{B}+\mathfrak{C})\subseteq\mathfrak{A}\mathfrak{B}+\mathfrak{A}\mathfrak{C}$. 另一方面，$ab=a(b+0)\in\mathfrak{A}(\mathfrak{B}+\mathfrak{C})$，故 $\mathfrak{A}\mathfrak{B}\subseteq\mathfrak{A}(\mathfrak{B}+\mathfrak{C})$. 同理，$\mathfrak{A}\mathfrak{C}\subseteq\mathfrak{A}(\mathfrak{B}+\mathfrak{C})$. 于是，$\mathfrak{A}\mathfrak{B}+\mathfrak{A}\mathfrak{C}\subseteq\mathfrak{A}(\mathfrak{B}+\mathfrak{C})$. 故 $\mathfrak{A}(\mathfrak{B}+\mathfrak{C})=\mathfrak{A}\mathfrak{B}+\mathfrak{A}\mathfrak{C}$. 同样論証可应用于建立另一个分配律.

一个子羣的冪可由 $\mathfrak{A}^1=\mathfrak{A}$, $\mathfrak{A}^k=(\mathfrak{A}^{k-1})\mathfrak{A}$ 来归納地定义. $\mathfrak{A}^k$

易知是形状如 $a_1a_2\cdots a_k$ 的积之有限和的集合，这里 $a_i\in\mathfrak{A}$. 加法羣的一个子羣 $\mathfrak{A}$ 决定一个子环必須而且只須 $\mathfrak{A}$ 对于乘法封閉. 这个条件可用乘法表出如 $\mathfrak{A}^2\subseteq\mathfrak{A}$. 子羣 $\mathfrak{B}$ 是环 $\mathfrak{R}$ 的一个理想的条件是

(L) $$\mathfrak{R}\mathfrak{B}\subseteq\mathfrak{B},$$

(R) $$\mathfrak{B}\mathfrak{R}\subseteq\mathfrak{B}.$$

环論里，子羣只适合上面两个条件中的一个时，很为重要. 如果 $\mathfrak{B}$ 是一个子羣使 (L) 成立，則 $\mathfrak{B}$ 叫做 $\mathfrak{R}$ 的左理想；如果 (R) 成立，則 $\mathfrak{B}$ 叫做右理想.

例. 令 $\mathfrak{R}_n$ 是由环 $\mathfrak{R}$ 定义的陣环. 今考究 $\mathfrak{R}_n$ 里由形状如

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2k} & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nk} & 0 & \cdots & 0 \end{bmatrix}$$

的陣构成的子集合 $\mathfrak{B}$，这里 a_{ij} 是任意的，則 $\mathfrak{B}$ 是一个左理想. 仿此，由下方 $n-k$ 行都是 0 的陣的全部构成的子集合是 $\mathfrak{R}_n$ 里一个右理想. 我們可証：这两个集合中无一个是(双側)理想.

在任一个环 $\mathfrak{A}$ 里，左倍数 xb 的全部 $\mathfrak{A}b$ 是一个左理想，这里 $x\in\mathfrak{A}$. 如果 $\mathfrak{A}$ 含有一个恆等元素，則 $\mathfrak{A}b$ 含有 b，并且 $\mathfrak{A}b$ 的特性是含有 b 的左理想里的最小者. 这因为，$\mathfrak{A}b$ 显然是被包含于每个含有 b 的左理想里. 如果 $\mathfrak{A}$ 沒有恆等元素，則它必須取形状如 $nb+xb$ 的元素的集合，才能得到包含 b 的最小左理想的目的，这里 n 是整数，x 是 $\mathfrak{A}$ 里任意元素. 我們把这含有元素 b 的最小左理想叫做主左理想，記作 $(b)_l$. 于是，当 $\mathfrak{A}$ 含有恆等元素时，$(b)_l=\mathfrak{A}b$；而 $\mathfrak{A}$ 是任意时，$(b)_l$ 是集合 $\{nb+xb\}$. 同理可定义 b 的右倍数的右理想 $b\mathfrak{A}$，及主右理想 $(b)_r$. 我們常有 $(b)_r\supseteq b\mathfrak{A}$；但 $\mathfrak{A}$ 拥有恆等元素时，則 $(b)_r=b\mathfrak{A}$.

单側理想的概念可用以得出除环的一个新特性：

定理 8. 帶恆等元素 $1\neq 0$ 的环是一个除环，必須而且只須它沒有眞左(右)理想.

証 先設 $\mathfrak{A}$ 是一个除环. 如果 $\mathfrak{B}$ 是 $\mathfrak{A}$ 里一个左理想，$\neq 0$，則

$\mathfrak{B}$含有一个元素 $b \neq 0$. 于是, $1 = b^{-1}b \in \mathfrak{B}$, 而且每个 $x = x1 \in \mathfrak{B}$. 所以, $\mathfrak{B} = \mathfrak{A}$. 故若 $\mathfrak{B}$ 是任一个左理想, 则或者 $\mathfrak{B} = 0$, 或者 $\mathfrak{B} = \mathfrak{A}$. 反过来, 令 $\mathfrak{A}$ 是带恆等元素 $1 \neq 0$ 的环, 它沒有眞左理想. 如果 b 是 $\mathfrak{A}$ 里 $\neq 0$ 的一个元素, 則 $\mathfrak{A}b$ 含有 $1b \neq 0$. 故 $\mathfrak{A}b = \mathfrak{A}$. 由此可知有 $c(\neq 0)$ 存在, 使 $cb = 1$. 故 $\neq 0$的每个元素有一个左逆元素 $\neq 0$. 由此可見, $\mathfrak{A}$ 的非零元素对于乘法成一个羣 (参看习題 8 的第 2 題). 故 $\mathfrak{A}$ 是一个除环.

由这个結果当然得出: 任一个除环是单純环. 故一个除环的唯一同态象是 0 及它自身.

我們可驗証: 把交, 和及积等合成使用于左 (右) 理想得出左 (右) 理想. 这类型的其它結果也可建立. 例如, 如果 $\mathfrak{B}$是任一个左理想, 而 $\mathfrak{C}$ 是一个子羣, 則积 $\mathfrak{B}\mathfrak{C}$ 是一个左理想. 又若 $\mathfrak{B}$ 是一个左理想, 而 $\mathfrak{C}$ 是一个右理想, 則 $\mathfrak{B}\mathfrak{C}$ 是一个(双側)理想.

习 題 35

1. 求証: 不含有眞左理想的环 $\mathfrak{A}$ 或者是一个除环, 或者是一个零环.
2. 如果 $\mathfrak{A}$ 是任一个环, 則 $\mathfrak{A}^2$, $\mathfrak{A}^3$, … 是理想. 如果 $\mathfrak{A}$ 是 I_3 里由形如

$$\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix}$$

的陣所构成的子环, 这些理想是什么?

13. 交換羣的自同态环

令 $\mathfrak{G}$ 是一个任意交換羣. 在 $\mathfrak{G}$ 里用加法記号 + 表合成, 0 表恆等元素, $-a$ 表 a 的逆元素, ma 表 a 的冪或倍数. 今考究 $\mathfrak{G}$ 的自同态的集合 $\mathfrak{E}$. 这些映照是 $\mathfrak{G}$ 到它自身内的映照 η, 它使

$$(a+b)\eta = a\eta + b\eta. \tag{22}$$

我們知道, 如果 $\eta, \rho \in \mathfrak{E}$, 則 $\eta\rho \in \mathfrak{E}$, 且結合律对于积合成是成立的. 我們还知道, 恆等映照属于 $\mathfrak{E}$. 縱使 $\mathfrak{G}$ 非交換羣, 这些結果也是成立的. 但在可交換情形下, 更大量的結果可以証出, 即我們可証: 集合 $\mathfrak{E}$ 可用以定义一个环.

在 $\mathfrak{E}$ 里引入加法合成, 而定义 $\eta + \rho$ 为

$$a(\eta + \rho) = a\eta + a\rho. \tag{23}$$

因为

$$(a+b)(\eta+\rho)=(a+b)\eta+(a+b)\rho$$
$$=a\eta+b\eta+a\rho+b\rho$$
$$=a\eta+a\rho+b\eta+b\rho$$
$$=a(\eta+\rho)+b(\eta+\rho),$$

故这映照是一个自同态. 不难験証: $\mathfrak{E}$, + 是一个交换羣. 这因为

$$a(\eta+(\rho+\lambda))=a\eta+a(\rho+\lambda)=a\eta+a\rho+a\lambda,$$
$$a((\eta+\rho)+\lambda)=a(\eta+\rho)+a\lambda=a\eta+a\rho+a\lambda;$$

故 $\eta+(\rho+\lambda)=(\eta+\rho)+\lambda$. 仿此得 $\eta+\rho=\rho+\eta$. 今把每个 a 映到 0 的映照定义为 0 映照, 显然这是一个自同态; 并且对于所有 η, $\eta+0=\eta$. 最后, 設 $\eta\in\mathfrak{E}$, 我們定义 $-\eta$ 为映照 $a\to-(a\eta)$; 这映照可看为 $a\to a\eta$ 与自同构 $a\to-a$ 的积. 故 $-\eta\in\mathfrak{E}$. 显然, $\eta+(-\eta)=0$.

設以 · 表变换的积, 今来証 $\mathfrak{E}$, +, · 是一个环. 这因为, 已知 $\mathfrak{E}$, + 是一个交换羣; 又因为知道 · 是結合性的; 所以只要証明分配律就够了. 因为

$$a(\eta(\rho+\lambda))=(a\eta)(\rho+\lambda)=(a\eta)\rho+(a\eta)\lambda$$
$$=a(\eta\rho)+a(\eta\lambda)=a(\eta\rho+\eta\lambda),$$

故 $\eta(\rho+\lambda)=\eta\rho+\eta\lambda$. 又因为

$$a((\rho+\lambda)\eta)=(a(\rho+\lambda))\eta=(a\rho+a\lambda)\eta$$
$$=(a\rho)\eta+(a\lambda)\eta=a(\rho\eta)+a(\lambda\eta)=a(\rho\eta+\lambda\eta),$$

故 $(\rho+\lambda)\eta=\rho\eta+\lambda\eta$. 这就証明了下面的基本定理.

定理 9. 令 $\mathfrak{G}$ 是一个任意交换羣(用加法寫出), 并令 $\mathfrak{E}$ 是 $\mathfrak{G}$ 的自同态的全部, 則 $\mathfrak{E}$ 关于由 $a(\eta+\rho)=a\eta+a\rho$ 定义的加法合成及关于積合成 · 是封閉的, 并且 $\mathfrak{E}$, +, · 是一个环.

$\mathfrak{E}$ 叫做 $\mathfrak{G}$ 的自同态环. 考究环 $\mathfrak{E}$ 的子环, 一般更多兴趣. 这样一个子环叫做一个自同态环. 在下一节可見, 这些环在环論上的地位有如变换羣在羣論上的地位. 在討論这个事实前, 我們先考究一些例子.

例. (1) $\mathfrak{G}$ 是一个无限循环羣，则可取 $\mathfrak{G}$ 为整数的加法羣 I_+. 設 $\eta\in\mathfrak{E}$，而 $1\eta=u\in I_+$. 因为 η 是一个自同态，故 $n\eta=nu$. 这段説明指出，η 是由它对于 I_+ 的生成元素 1 的效果所决定. 故我們可将整数 u (η 作用于 1 的效果) 与自同态 η 連結起来. 今設 ρ 是另一个自同态，而且 $1\rho=v$. 則可把 v 与 ρ 連結起来. 再則 $1(\eta+\rho)=1\eta+1\rho=u+v$ 及 $(1\eta)\rho=u\rho=uv$. 故在这对应下，$\eta+\rho\to u+v$ 及 $\eta\rho\to uv$. 这个对应是 1—1 的; 这因为，如果 $u=v$，则 $1\eta=1\rho$. 又因为一个自同态是由它对于 1 的作用效果来决定. 故 $\eta=\rho$. 于是，得从 $\mathfrak{E}$ 到整数的环 I 内的一个同构. 最后，我們知道，这同构是 $\mathfrak{E}$ 到 I 上的一个同构. 故如果 u 是任一个整数，则因

$$(n+m)u=nu+mu$$

是倍数的一个基本性质，故映照 $n\to nu$ 是一个自同态. 显然，这个自同态把 1 映到 u; 因此，就証明了 $\mathfrak{E}$ 与 I 同构.

(2) 次考究所有整向量 $(m_1, m_2, \cdots, m_n)$ 的羣 $\mathfrak{G}$，作为 (1) 的一个拓广，这里 $m_i\in I$. 我們用向量加法作合成. 如果引入向量

(24) $$e_i=(0,\cdots,0,\overset{i}{1},0,\cdots,0),\quad i=1,2,\cdots,n,$$

则得

(25) $$(m_1,m_2,\cdots,m_n)=m_1e_1+m_2e_2+\cdots+m_ne_n.$$

故任一个整向量是属于由 e_i 生成的羣里. 一个向量显然只能有一种方式写成 Σm_ie_i; 这因为，如果 $\Sigma m_ie_i=\Sigma m_i'e_i$，则由 (25) 有

$$(m_1, m_2, \cdots, m_n)=(m_1', m_2', \cdots, m_n'),$$

故对于所有 i, $m_i=m_i'$.

令 η 是 $\mathfrak{G}$ 里一个自同态. 今来驗証: η 可由它作用于 e_i 的效果而完全决定. 这因为，如果知道了象 $e_i\eta=f_i$，则象

$$(\Sigma m_ie_i)\eta=\Sigma(m_ie_i)\eta=\Sigma m_i(e_i\eta)=\Sigma m_if_i$$

也就知道. 所以，如果 η 与 ρ 是两个自同态，且 $e_i\eta=e_i\rho\ (i=1,2,\cdots,n)$，则对于所有 a 得 $a\eta=a\rho$; 于是，$\eta=\rho$.

次設

(26) $$f_i=e_i\eta=a_{i1}e_1+a_{i2}e_2+\cdots+a_{in}e_n,$$

这里 a_{ij} 是整数. 显然这些整数由 η 唯一决定. 故陣

$$(a_{ij})=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{bmatrix}$$

由 η 决定. 这个陣叫做 η 的陣. 我們将要考察从 $\mathfrak{E}$ 到元素属于 I 的 $n\times n$ 陣构成的环 I_n 内的对应 $\eta\to(a_{ij})$.

首先要説，这个对应是 1—1 的; 这因为，如果 $\eta\to(a_{ij})$ 及 $\rho\to(a_{ij})$，则 $e_i\eta=e_i\rho$，故 $\eta=\rho$. 其次，令 ρ 是任一个自同态，并令 $\rho\to(b_{ij})$. 则 $e_i\rho=\sum_j b_{ij}e_j$. 故

$$e_i(\eta+\rho)=e_i\eta+e_i\rho=\sum_j a_{ij}e_j+\sum_j b_{ij}e_j=\sum_j(a_{ij}+b_{ij})e_j.$$

因此，$\eta+\rho\to(a_{ij})+(b_{ij})$. 最后，

$$e_i(\eta\rho)=(e_i\eta)\rho=(\sum_j a_{ij}e_j)\rho=\sum_j(a_{ij}e_j)\rho=\sum_j a_{ij}(e_j\rho)=\sum_{j,k}a_{ij}b_{jk}e_k=\sum_k c_{ik}e_k,$$

这里 $c_{ik}=\sum_j a_{ij}b_{jk}$. 这指出，$\eta\rho$ 的陣是 $(a)(b)$. 故我們証明了: $\eta\to(a)$ 是 $\mathfrak{E}$ 到 I_n

內的一个同构.

最后，我們要指出，这映照是 $\mathfrak{E}$ 到 I_n 上的同构. 令 (a) 是 I_n 里任一个陣，并令 $f_i = \sum_j a_{ij}e_j$. 我們定义 $\mathfrak{G}$ 到它自身內的一个映照規定为 $\sum m_ie_i \to \sum m_if_i$. 所以，如果 $\sum m_i'e_i$ 是 $\mathfrak{G}$ 的另一个元素，則

$$\sum m_ie_i + \sum m_i'e_i = \sum(m_i + m_i')e_i,$$

且这个元素映到

$$\sum(m_i + m_i')f_i = \sum m_if_i + \sum m_i'f_i.$$

故 $\sum m_ie_i \to \sum m_if_i$ 是一个自同态 η. 因为 $e_i\eta = f_i = \sum a_{ij}e_j$, 故 η 的陣是給定的陣 (a). 所以，我們建立了 $\mathfrak{E}$ 到 I_n 上的一个同构.

我們可使用刚才引导出来以决定 $\mathfrak{G}$ 的自同构羣的結論. 显然，如果 $\mathfrak{G}$ 是任一个交換羣，則 $\mathfrak{G}$ 的自同构羣 $\mathfrak{A}$ 与环 $\mathfrak{E}$ 里单位元素羣重合. 如果我們有从一个环到另一个上的一个同构，則第一个环的单位元素羣必映到后一个的单位元素羣上，这也是显然的. 故我們可由决定陣环 I_n 的单位元素羣决定出整向量的羣 $\mathfrak{G}$ 的自同构羣. 今我們知道，陣 $(a) \in I_n$ 是 I_n 里一个单位元素必須而且只須 $\det(a) = \pm 1$. 把这个結果与上面討論合併起来，可見: $\mathfrak{G}$ 的自同构的形状如 $\sum m_ie_i \to \sum m_if_i$, 这里 $f_i = \sum a_{ij}e_j$, 而且 $\det(a) = \pm 1$.

习 題 36

1. 决定 n 阶循环羣的自同态环及自同构羣.

2. 令 $\mathfrak{G}$ 是一个任意羣，并令 $\mathfrak{M}$ 是 $\mathfrak{G}$ 到它自身內的全部映照的集合. 如果 $\eta, \rho \in \mathfrak{M}$, 定义 $\eta\rho$ 是它們的积，而 $\eta + \rho$ 为 $g(\eta + \rho) = (g\eta)(g\rho)$. 求考究关于这两个合成的集合 $\mathfrak{M}$.

14. 环的乘法

今設 $\mathfrak{A}$ 是任一个环. 如果 a 是 $\mathfrak{A}$ 的一个固定元素，我們定义 $\mathfrak{A}$ 到它自身內的映照 $x \to xa$ 为右乘变換 a_r. 因

$$(x + y)a_r = (x + y)a = xa + ya = xa_r + ya_r, \tag{27}$$

故这映照是 $\mathfrak{A}$ 的加法羣 $\mathfrak{A}, +$ 的一个自同态. 次因为

$$x(a + b)_r = x(a + b) = xa + xb = xa_r + xb_r = x(a_r + b_r),$$

及

$$x(ab)_r = x(ab) = (xa)b = (xa_r)b_r = x(a_rb_r),$$

故得关系

$$\begin{aligned}(a + b)_r &= a_r + b_r,\\ (ab)_r &= a_rb_r.\end{aligned} \tag{28}$$

这証明: 对应 $a \to a_r$ 是环 $\mathfrak{A}$ 到 $\mathfrak{A}, +$ 的自同态环 $\mathfrak{E}$ 內的一个同态. 故右乘变換的集合 $\mathfrak{A}_r$ 当然是 $\mathfrak{E}$ 的一个子环. 我們叫做环 $\mathfrak{A}$ 的右乘变換环.

同态 $a \to a_r$ 的核是元素 z 的理想 $\mathfrak{Z}_r$, 这 z 对于所有 x 会使

$xz = 0$ 的．这理想叫做环 $\mathfrak{A}$ 的右零化子．設 $\mathfrak{Z}_r = 0$，我們知道，$a \rightarrow a_r$ 是一个同构．其特款为，在 $\mathfrak{A}$ 拥有恆等元素的重要情形下，$\mathfrak{Z}_r = 0$；这因为，如果 $1z = 0$，則 $z = 0$．下面基本定理就是作为一个推理而被証明的．

定理 10. 帶有恆等元素的任一个环与自同态环是同構的[1]．

类似討論可应用于由 $xa_l = ax$ 定义的左乘变换 a_l．这些映照都是自同态，且适合

(29) $$(a + b)_l = a_l + b_l, \quad (ab)_l = b_l a_l.$$

故 $a \rightarrow a_l$ 是 $\mathfrak{A}$ 到 $\mathfrak{E}$ 内的一个反同态(参看习題 33 的第 5 題)．故象集合，亦即左乘变换的集合 $\mathfrak{A}_l$，是 $\mathfrak{E}$ 的一个子环．反同态 $a \rightarrow a_l$ 的核是环 $\mathfrak{A}$ 的左零化子的理想 $\mathfrak{Z}_l$．如果 $\mathfrak{A}$ 有恆等元素，則 $\mathfrak{Z}_l = 0$，并且 $a \rightarrow a_l$ 是一个反同构．

最后，我們考究带恆等元素环的左乘及右乘变換間的一个重要关系，写成下面的定理：

定理 11. 如果 $\mathfrak{A}$ 是帶恆等元素环，則 $\mathfrak{A}, +$ 里能夠与所有左(右)乘变換相交換的任一个变換必是一个右(左)乘变換．

这定理的証明与第 1 章的 §10 里关于羣的对应証明完全相同．

1) 在下一章中，将証这結果对于不拥有恆等元素的环也成立．——著者注．

第 三 章

环 及 域 的 扩 张

一个給定的环会缺乏解特殊問題所需要的某些性質．但我們能作一个較大的环，使它具备所需要的性質．例如，存在有形状如 $ax = b(a \neq 0)$ 的方程，它在整数的整区里无解；而作有理数域的目的卽保証这类型方程的可解性．作这样扩张所用的方法可以推广而用于任一个交換整区．这种类型的扩张是本章所討論各种扩张的一种．在其它类型的扩张中，我們还定义多項式环、域扩张及函数环．我們导出这些扩张的某些性質；特别是决定任一个域的代数結构．

1. 把一个环嵌入于带恒等元素环　前章里已証明带恆等元素的任一个环与自同态环同构．今将証明：任一个环 $\mathfrak{A}$ 必与带恆等元素环 $\mathfrak{B}$ 的一个子环 $\mathfrak{A}'$ 同构．因为 $\mathfrak{B}$ 与一个自同态环同构，故 $\mathfrak{A}'$ 与一个自同态环同构，从而 $\mathfrak{A}$ 也是如此．

一般来說，如果一个环 $\mathfrak{B}$ 含有与环 $\mathfrak{A}$ 同构的一个子环，則說：$\mathfrak{A}$ 被嵌入于 $\mathfrak{B}$ 內，而环 $\mathfrak{B}$ 叫做 $\mathfrak{A}$ 的一个扩张．

要作 $\mathfrak{A}$ 的一个扩张，使它带有恆等元素，可令 $\mathfrak{B}$ 为二維組 (m, a) 的积集合 $I \times \mathfrak{A}$，这里 m 是一个整数，而 a 属于給定的环 $\mathfrak{A}$ 里．两个二維組 (m, a) 及 (n, b) 認为相等，必須而且只須 $m = n$ 及 $a = b$．我們在 $\mathfrak{B}$ 里以

(1)　　$$(m, a) + (n, b) = (m + n, a + b)$$

定义加法合成．容易看出，$\mathfrak{B}$，+ 是一个交換羣，0 元素是 $(0, 0)$，而 $-(m, a) = (-m, -a)$．又在 $\mathfrak{B}$ 里以

(2)　　$$(m, a)(n, b) = (mn, na + mb + ab)$$

定义乘法，这里右端的 na 及 mb 分別表 a 的 n 倍及 b 的 m 倍．因

为

$$((m, a)(n, b))(q, c) = ((mn)q, q(na) + q(mb) + q(ab) + (mn)c + (na)c + (mb)c + (ab)c)$$

及

$$(m, a)((n, b)(q, c)) = (m(nq), m(nc) + m(qb) + m(bc) + a(nq) + a(nc) + a(qb) + a(bc)),$$

故由 $\mathfrak{A}$ 及 I 里倍数、加法的交换律及結合律各性质推得 $\mathfrak{B}$ 里乘法的結合律. 又因为

$$\begin{aligned}(m, a)[(n, b) + (q, c)] &= (m, a)(n + q, b + c) \\ &= (m(n + q), m(b + c) + (n + q)a + a(b + c)) \\ &= (mn + mq, mb + mc + na + qa + ab + ac)\end{aligned}$$

及

$$\begin{aligned}&(m, a)(n, b) + (m, a)(q, c) \\ &= (mn, mb + na + ab) + (mq, mc + qa + ac) \\ &= (mn + mq, mb + na + ab + mc + qa + ac),\end{aligned}$$

故两个分配律中的一个成立. 仿此可驗証另一个分配律也成立. 故这样作出的代数系成一个环.

由使用(2)可見,元素 $1 = (1, 0)$ 在 $\mathfrak{B}$ 里有恆等元素的作用. 次考虑 $\mathfrak{B}$ 里形状如 $(0, a)$ 的元素的集合 $\mathfrak{A}'$. 因为

$$(0, a) + (0, b) = (0, a + b), \quad 0 = (0, 0),$$
$$-(0, a) = (0, -a), \text{ 及 } (0, a)(0, b) = (0, ab),$$

故 $\mathfrak{A}'$ 是 $\mathfrak{B}$ 的一个子环. 如果命 $a' = (0, a)$, 我們还显見, 对应 $a \to a'$ 是 $\mathfrak{A}$ 到 $\mathfrak{A}'$ 上的一个同构. 故 $\mathfrak{A}$ 被嵌入于带恆等元素环 $\mathfrak{B}$ 內. 这証明了下面的定理.

定理 1. 任一个环可被嵌入于一个帶恆等元素环內.

由于映照 $m \to (m, 0)$是 I 到 $\mathfrak{B}$ 的一个子环 I' 上的一个同构, 所以我們也可說,整数环被嵌入于环 $\mathfrak{B}$ 內. 今以 m 代 $(m, 0)$, a 代 $(0, a)$, I 代 I', $\mathfrak{A}$ 代 $\mathfrak{A}'$,使記法簡单. 使用这些記法,得关系

$$\mathfrak{B} = I + \mathfrak{A}, \quad I \cap \mathfrak{A} = 0.$$

显然, $\mathfrak{A}$ 是 $\mathfrak{B}$ 里一个理想.

注意. 在某些情况下，$\mathfrak{B}$ 不能作为 $\mathfrak{A}$ 扩张到带恆等元素环的最适用的扩张. 首先是，如果一开始 $\mathfrak{A}$ 就拥有恆等元素 e，则元素 $z = 1 - e$ 对于 $\mathfrak{A}$ 里所有 a 具有性质 $za = 0 = az$. 故在这个情形下，就不值得引入环 $\mathfrak{B}$. 其次要講的是，$\mathfrak{B}$ 的特征数可与 $\mathfrak{A}$ 的特征数不同. 这种情形出現于 $\mathfrak{A}$ 的特征数是 $m \neq 0$. 此时，由于 $\mathfrak{B} \supseteq I$，故 $\mathfrak{B}$ 的特征数是 0. 但我們容易由修改作法，得出带恆等元素的一个扩张，使它的特征数与 $\mathfrak{A}$ 的特征数相同. 这在下面习題 37 的第 1 題中指出. 上述作法的另一个缺点为：$\mathfrak{A}$ 是一个整区，但 $\mathfrak{B}$ 可以不是一个整区. 例如，設 $\mathfrak{A}$ 是偶整数的环，則 $\mathfrak{B}$ 的元素 $(2, -2)$ 具有性质 $(2, -2)(0, 2m) = 0$. 这种困难是可以克服的，并且我們可証：任一个整区可被嵌入于带恆等元素的一个整区內. 下面习題的第 2—4 題就是意图建立这个結果.

习 題 37

1. 如果 $\mathfrak{A}$ 是一个环，对于它的所有元素 a 存在一个正整数 m，使 $ma = 0$. 令 $\mathfrak{C}$ 表二維組 $(\bar{n}, a)$ 的集合，这里 $\bar{n} = n + (m)$ 是环 $I/(m)$ 的元素. 沿用課文中所述关于环 $\mathfrak{B}$ 里相等的定义，但定义加法为

$$(\bar{n}, a) + (\bar{q}, b) = (\bar{n} + \bar{q}, a + b),$$

定义乘法为

$$(\bar{n}, a)(\bar{q}, b) = (\bar{n}\bar{q}, nb + qa + ab).$$

求驗証：乘法是单值的，并且 $\mathfrak{C}$ 是带恆等元素环，它是 $\mathfrak{A}$ 的一个扩张，且对于所有 $c \in \mathfrak{C}$, $mc = 0$.

2. 如果 $\mathfrak{A}$ 是一个整区，它含有元素 a 及 $b \neq 0$，使对于某个整数 m 有 $ab + mb = 0$，求証：对于所有 $c \in \mathfrak{A}$，

$$ca + mc = 0 = ac + mc.$$

3. 如果 $\mathfrak{A}$ 是一个整区，并令 $\mathfrak{B}$ 是課文中所作的环. 驗証：对于所有 $a \in \mathfrak{A}$，能使 $za = 0$ 的 $\mathfrak{B}$ 里元素 z 的全部 $\mathfrak{Z}$ 是一个理想，并且 $\mathfrak{B}/\mathfrak{Z}$ 是带恆等元素的一个整区.

4. 求証：$a \in \mathfrak{A}$ 时，形状如 $a + \mathfrak{Z}$ 的陪集的集合 $\bar{\mathfrak{A}}$ 是 $\mathfrak{B}/\mathfrak{Z}$ 的一个子环，与 $\mathfrak{A}$ 同构. 故 $\mathfrak{A}$ 被嵌入于 $\mathfrak{B}/\mathfrak{Z}$ 內.

2. 交換整区的分式域 今要指出任一个交換整区可被嵌入于一个域內. 我們要講的作法，在整数环情形已是众所熟知的. 这作法可由考究域的一个子环与由子环生成的子域間的关系而得到深入的了解.

因此，令 $\mathfrak{F}$ 是一个域，并令 $\mathfrak{A}$ 是 $\mathfrak{F}$ 的一个子环，$\neq 0$. 如果代数系 $\mathfrak{A}, +, \cdot$ 是一个域，則說 $\mathfrak{A}$ 是 $\mathfrak{F}$ 的一个子域. 由此可見：域

$\mathfrak{F}$ 的一个子集合 $\mathfrak{A}$ 决定一个子域必須而且只須 (1) $\mathfrak{A}$, + 是加法羣的一个子羣; (2) $\mathfrak{A}$ 含有元素 $\neq 0$; 如果令 $\mathfrak{A}^*$ 表这些非零元素的全部,則 $\mathfrak{A}^*$, · 是 $\mathfrak{F}$ 的非零元素的乘法羣的一个子羣. 回忆羣的一个子集合决定一个子羣的条件,可見: $\mathfrak{A}$ 决定一个子域必須而且只須

1′. 如果 $a, b \in \mathfrak{A}$,則 $a+b \in \mathfrak{A}$. $0 \in \mathfrak{A}$. 如果 $a \in \mathfrak{A}$,則 $-a \in \mathfrak{A}$.

2′. $1 \in \mathfrak{A}$. 如果 a 及 b 是 $\mathfrak{A}$ 的非零元素,則 ab 及 $a^{-1} \in \mathfrak{A}$.

由 1′ 及 2′ 显然知,由一个域的子域組成的任一个集合的交还是一个子域.如果 S 是 $\mathfrak{F}$ 的任一个子集合,則 $\mathfrak{F}$ 里含有 S 的所有子域的交,叫做 $\mathfrak{F}$ 里含 S 的最小子域,或 $\mathfrak{F}$ 里由 S 生成的子域. 今来叙述下面的重要观察: 如果 $S = \mathfrak{A}$ 是 $\mathfrak{F}$ 的一个子环, $\neq 0$, 則由 $\mathfrak{A}$ 生成的子域 $\mathfrak{G}$ 与形状如 ab^{-1} 的元素的集合 $\{ab^{-1}\}$ 重合, 这里 a, $b \in \mathfrak{A}$. 这因为,显然 $\mathfrak{G} \supseteq \{ab^{-1}\}$. 再則我們有下面各等式:

$$ab^{-1} + cd^{-1} = adb^{-1}d^{-1} + cbb^{-1}d^{-1} = (ad + cb)(bd)^{-1},$$
$$0 = 0\,b^{-1},$$
$$-ab^{-1} = (-a)b^{-1},$$
$$(ab^{-1})(cd^{-1}) = acb^{-1}d^{-1} = (ac)(bd)^{-1},$$
$$1 = aa^{-1} \quad (a \neq 0),$$
$$(ab^{-1})^{-1} = a^{-1}b \quad (a \neq 0),$$

它們指出集合 $\{ab^{-1}\}$ 决定一个子域. 因为 $\mathfrak{A}$ 里任一个 a 可写成

$$a = (ab)b^{-1},$$

故 $\mathfrak{A} \subseteq \{ab^{-1}\}$. 于是,集合 $\{ab^{-1}\}$ 是 $\mathfrak{F}$ 里含有 $\mathfrak{A}$ 的一个子域. 因为 $\mathfrak{G} \supseteq \{ab^{-1}\}$, 故推得 $\mathfrak{G} = \{ab^{-1}\}$.

如果 $\mathfrak{F} = \mathfrak{G}$,則說 $\mathfrak{F}$ 是包含 $\mathfrak{A}$ 的极小域. 此时易知 $\mathfrak{F}$ 的每个元素的形状为 ab^{-1}, 这里 $a, b \in \mathfrak{A}$.

今設 $\mathfrak{A}$ 是任一个非零交換整区, 而企图把 $\mathfrak{A}$ 扩张为域. 上面的討論指出: $\mathfrak{A}$ 的一个极小域扩张的各元素是从二維組 (a, b) 得来, 这里 $a, b \in \mathfrak{A}$, $b \neq 0$. 我們心中記住: (a, b) 是承担 ab^{-1} 的任务;因此采取下面的步驟.

令 $\mathfrak{B}$ 是二維組 (a, b) 的全部,这里 $a, b \in \mathfrak{A}$, $b \neq 0$. 于 $\mathfrak{B}$ 里

引入一个关系，定义为：如果 $ad = bc$，則 $(a, b) \sim (c, d)$. 因为 $ab = ba$，故 $(a, b) \sim (a, b)$. 次設 $(a, b) \sim (c, d)$，則 $ad = bc$，从而 $cb = da$，故 $(c, d) \sim (a, b)$. 末了，設 $(a, b) \sim (c, d)$ 及 $(c, d) \sim (e, f)$，則 $ad = bc$，及 $cf = de$；于是，$adf = bcf = bde$. 因为 $d \neq 0$，而 $\mathfrak{A}$ 是可交換的，故 d 可相消，而得 $af = be$；于是，$(a, b) \sim (e, f)$. 这証明了关系 $\sim$ 是 $\mathfrak{B}$ 里一个等价关系. 由 (a, b) 决定的等价类叫做**分式**，記作 a/b. 故得法則：

$$a/b = c/d \text{ 必須而且只須 } ad = bc.$$

今在分式集合 $\mathfrak{F}$ 里引入加法与乘法合成. 首先要說的是：如果 a/b 及 c/d 是任两个分式，則 $bd \neq 0$，且可作分式 $(ad + bc)/bd$. 其次，如果 $a/b = a'/b'$ 及 $c/d = c'/d'$，則

$$(ad + bc)/bd = (a'd' + b'c')/b'd'. \tag{3}$$

这因为由假設得 $ab' = ba'$ 及 $cd' = dc'$. 于是，

$$ab'dd' = ba'dd' \text{ 及 } cd'bb' = dc'bb'.$$

因此得

$$ab'dd' + cd'bb' = ba'dd' + dc'bb',$$

或

$$(ad + bc)b'd' = (a'd' + b'c')bd,$$

这与(3)等价. 由此显見：用

$$a/b + c/d = (ad + bc)/bd \tag{4}$$

定义的加法合成在 $\mathfrak{F}$ 里是一个单值合成. 同理可知：如果 a/b 及 c/d 是分式，則 ac/bd 是一个分式. 如果 $a/b = a'/b'$ 及 $c/d = c'/d'$，則 $ac/bd = a'c'/b'd'$. 故

$$(a/b)(c/d) = ac/bd \tag{5}$$

定义一个单值乘法.

我們还可直接驗証：集合 $\mathfrak{F}$ 連同合成(4)及(5)成一个交換环. 这手續让讀者来做. 此外还可得到：$0/b = 0/d$ 是 $\mathfrak{F}$ 里的 0，而 a/b 的負元素是 $(-a)/b = a/(-b)$. 环 $\mathfrak{F}$ 拥有恒等元素. 这因为，对于任一个 $b \neq 0$ 及 $d \neq 0$，$b/b = d/d$，并且 $(a/b)(b/b) = ab/b^2 = a/b$. 故 $b/b = 1$. 如果 $a/b \neq 0$，則 $a \neq 0$，故 b/a 是一

个分式. 因为 $(a/b)(b/a)=ab/ba=1$, 故 $b/a=(a/b)^{-1}$. 这指出 $\mathfrak{F}$ 里每个非零元素都是单位元素. 故 $\mathfrak{F}$ 是一个域.

今将 $\mathfrak{A}$ 的元素 a 与分式 ab/b 联系起来,这里 b 是 $\mathfrak{A}$ 里任一个非零元素. 因为对于任一个 $d\neq 0$, $ab/b=ad/d$, 故这个对应是单值的. 設以 $\bar{a}$ 表示 ab/b, 则

$$\begin{aligned}\overline{a+a'}&=(a+a')b/b=(a+a')b^2/b^2\\&=(ab^2+a'b^2)/b^2=ab/b+a'b/b=\bar{a}+\bar{a}',\end{aligned}$$

及

$$\overline{aa'}=aa'b/b=aa'b^2/b^2=(ab/b)(a'b/b)=\bar{a}\bar{a}'.$$

故 $a\to\bar{a}$ 是一个同态. 我們还可直接驗証这映照是 1—1 的. 于是,元素 $\bar{a}$ 的集合 $\bar{\mathfrak{A}}$ 决定 $\mathfrak{F}$ 的一个子环,与 $\mathfrak{A}$ 是同构的. 这就証明了关于嵌入的下面基本定理:

定理 2. 任一个非零交换整区可被嵌入于一个域内.

今来說明: $\mathfrak{F}$ 是含有 $\mathfrak{A}$ 的象 $\bar{\mathfrak{A}}$ 的一个极小域. 这因为, $\mathfrak{F}$ 的任一个 a/b 显然可写成

$$a/b=(ab/b)(b/b^2)=(ab/b)(b^2/b)^{-1}=\bar{a}\bar{b}^{-1}.$$

如果 $\mathfrak{A}=$ 整数环 I, 则分式叫做**有理数**. 有理数域此后記作 R_0.

习 題 38

1. 如果 $\mathfrak{A}$ 是一个域,驗証: $\mathfrak{F}=\bar{\mathfrak{A}}$.
2. 求証:适合相消律的任一个交换半羣可被嵌入于一个羣内.

两个拓广 (1)刚才所用的方法可予拓广,以証: 含有由非零因子的元素所成非空集合 S 的任一个交换环 $\mathfrak{A}$ 可被嵌入于一个带恆等元素环内,而以 S 的元素为单位元素.

首先要說的是:如果 s_1s_2 是一个零因子,则 s_1 或者 s_2 必是一个零因子. 故 $\mathfrak{A}$ 的乘法半羣里,由給定的集合 S 生成的子半羣 V 不含零因子. 今考究二維組 (a, v) 的集合 $\mathfrak{A}\times V$, $a\in\mathfrak{A}$, $v\in V$, 并引入关系～:如果 $av'=a'v$, 则 $(a, v)\sim(a', v')$. 因为 V 不含零因子,故这关系是一个等价关系. 令 $\mathfrak{F}_S=\mathfrak{F}_V$ 是由这关系决定的等价类 a/v 的集合, 加法及乘法即用上面的定义, 这样就得一个

环，它含有一个子环 $\bar{\mathfrak{A}} \cong \mathfrak{A}$. $\bar{\mathfrak{A}}$ 的元素是类 $\bar{a} = av/v$. 环 $\mathfrak{F}_S$ 是可交换的，且有恆等元素 v/v. 如果 $s \in S$，则对应元素 $\bar{s} = sv/v$ 是 $\mathfrak{F}_S$ 里一个单位元素；它的逆元素是 v/sv.

(2) 有一类重要的非交换整区存在，它可被嵌入于除环内，这些就是拥有**公倍性质**的整区. 此时，在这种整区里，任两个非零元素 a, b 都有一个公右(左)倍 $m = ab' = ba' \neq 0$ $(\bar{m} = \bar{b}a = \bar{a}b \neq 0)$. 这类型整区的嵌入問題首由奧尔(O. Ore)解决. 他的作法与用于交换整区的作法相似；讀者欲知其詳，可參看 Ore 的論文[1].

最后，我們要提醒讀者，馬里茨夫 (A. Malcev) 曾証得：不能被嵌入在除环内的非交换整区也是存在的[2].

3. 分式域的唯一性 令 $\mathfrak{A}$ 是一个交換整区，并令 $\mathfrak{F}$ 是它的分式域. 今把 $\mathfrak{A}$ 与元素 $\bar{a} = ab/b$ 的子环 $\bar{\mathfrak{A}}$ 看作同一的代数系；因此，就可把 $\bar{\mathfrak{A}}$ 写作 $\mathfrak{A}$，把 $\bar{a}$ 写作 a. 于是，$\mathfrak{F}$ 里由 $\mathfrak{A}$ 生成的子域就是 $\mathfrak{F}$ 自身. 今将証明：与 $\mathfrak{A}$ 有这个关系的任意两个域必是同构的. 更确切地說，我們有下面的定理.

定理 3. 令 $\mathfrak{A}_i (i = 1, 2)$ 是域 $\mathfrak{F}_i$ 的一个非零子环，並設 $\mathfrak{F}_i$ 是含有 $\mathfrak{A}_i$ 的最小子域. 如果 σ 是 $\mathfrak{A}_1$ 到 $\mathfrak{A}_2$ 上的一个同構，则 σ 可有而且只有一种扩張成为 $\mathfrak{F}_1$ 到 $\mathfrak{F}_2$ 上的一个同構.

一个集合的一个映照**扩张成**为較大集合的一个映照是指較大集合上一个映照，它施于原来集合里各元素的效果与原来映照的效果相同. 故我們要求 $\mathfrak{F}_1$ 到 $\mathfrak{F}_2$ 上一个同构 Σ 对于所有 $a_1 \in \mathfrak{A}_1$ 能使 $a_1^\Sigma = a_1^\sigma$. 今将驗証：映照

$$(6) \qquad a_1 b_1^{-1} \to a_1^\sigma (b_1^\sigma)^{-1}, \quad b_1 \in \mathfrak{A}_1, \quad b_1 \neq 0,$$

就具有所要求的性質. 首先，因为 $\mathfrak{F}_1$ 对于 $\mathfrak{A}_1$ 是极小域，故 $\mathfrak{F}_1$ 的任一个元素的形状为 $a_1 b_1^{-1}$. 于是，(6) 对于整个 $\mathfrak{F}_1$ 是确定的. 次则 (6) 是单値的. 这因为，假設 $a_1 b_1^{-1} = c_1 d_1^{-1}$，則 $a_1 d_1 = c_1 b_1$，并且

---

1) 奥尔：非交换域里的綫性方程(Linear equations in non-commutative fields)，載在美国数学記录 (Annals of Math.)，卷32(1931)，463—477頁.——著者注.

2) 馬里茨夫：把一个代数环嵌入于域里(On the immersion of an algebraic ring in a field)，載在德国数学記录 (Mathematische Annalen)，卷 113 (1936)，686—691 頁. ——著者注.

$a_1^\sigma d_1^\sigma = c_1^\sigma b_1^\sigma$. 于是，$a_1^\sigma(b_1^\sigma)^{-1} = c_1^\sigma(d_1^\sigma)^{-1}$，即为所求. 同理可知：如果 $a_1^\sigma(b_1^\sigma)^{-1} = c_1^\sigma(d_1^\sigma)^{-1}$，则 $a_1b_1^{-1} = c_1d_1^{-1}$；故这映照是 1—1 的. 如果 $a_2b_2^{-1}$ 是 $\mathfrak{F}_2$ 的任一个元素，则可求得一个 a_1 使 $a_1^\sigma = a_2$，及一个 b_1 使 $b_1^\sigma = b_2$；于是，$a_2b_2^{-1} = a_1^\sigma(b_1^\sigma)^{-1}$ 是一个象. 故知这映照是 $\mathfrak{F}_1$ 到 $\mathfrak{F}_2$ 上的一个映照. 最后，因为

$$\begin{aligned} a_1b_1^{-1} + c_1d_1^{-1} &= (a_1d_1 + c_1b_1)(b_1d_1)^{-1} \\ &\to (a_1d_1 + c_1b_1)^\sigma((b_1d_1)^\sigma)^{-1} \\ &= (a_1^\sigma d_1^\sigma + c_1^\sigma b_1^\sigma)(b_1^\sigma d_1^\sigma)^{-1} \\ &= a_1^\sigma(b_1^\sigma)^{-1} + c_1^\sigma(d_1^\sigma)^{-1}, \end{aligned}$$

及

$$\begin{aligned} (a_1b_1^{-1})(c_1d_1^{-1}) = a_1c_1(b_1d_1)^{-1} &\to (a_1c_1)^\sigma((b_1d_1)^\sigma)^{-1} \\ &= (a_1^\sigma c_1^\sigma)(b_1^\sigma d_1^\sigma)^{-1} \\ &= (a_1^\sigma(b_1^\sigma)^{-1})(c_1^\sigma(d_1^\sigma)^{-1}). \end{aligned}$$

故为 $\mathfrak{F}_1$ 到 $\mathfrak{F}_2$ 上的一个同构. 因为这个同构把 $a_1 = (a_1b_1)b_1^{-1}$ 映到

$$(a_1b_1)^\sigma(b_1^\sigma)^{-1} = a_1^\sigma b_1^\sigma(b_1^\sigma)^{-1} = a_1^\sigma,$$

所以它是 σ 的一个扩张.

今設 Σ 是 $\mathfrak{F}_1$ 到 $\mathfrak{F}_2$ 上的任一个同构，它在 $\mathfrak{A}_1$ 里与 σ 的效果一致，则

$$(a_1b_1^{-1})^\Sigma = a_1^\Sigma(b_1^{-1})^\Sigma = a_1^\Sigma(b_1^\Sigma)^{-1} = a_1^\sigma(b_1^\sigma)^{-1}.$$

故 Σ 是映照 (6). 这指出：σ 的扩张成为 $\mathfrak{F}_1$ 到 $\mathfrak{F}_2$ 上的同构是唯一决定的. 定理就完全証明了.

4. 多項式环 我們对于研究含有一个特定子环 $\mathfrak{A}$ 的环 $\mathfrak{B}$ 常感兴趣. 将来就会知道，这观念在域論里特別多見. 在目前，一个自然的問題是：决定由 $\mathfrak{A}$ 及属于 $\mathfrak{B}$ 的另一个元素 u 所生成的一个子环 $\mathfrak{A}[u]$ 的結构. 为着簡化这个問題，假定：(1) $\mathfrak{B}$ 拥有恆等元素 1，(2) $1 \in \mathfrak{A}$，(3) 对于所有 $a \in \mathfrak{A}$，有 $ua = au$. 形状如

$$a_0 + a_1u + a_2u^2 + \cdots + a_nu^n, \quad a_i \in \mathfrak{A} \tag{7}$$

的任一个元素显然属于 $\mathfrak{A}[u]$. 我們叫它做 u 的多項式，它的系数 $a_i \in \mathfrak{A}$.

如果 $b_0 + b_1u + b_2u^2 + \cdots + b_mu^m$ 是又一个 u 的多項式，且

$n \geqslant m$，则

$$(8)\qquad \begin{aligned}&(a_0 + a_1u + a_2u^2 + \cdots + a_nu^n)\\ &\quad + (b_0 + b_1u + b_2u^2 + \cdots + b_mu^m)\\ &= (a_0 + b_0) + (a_1 + b_1)u + \cdots\\ &\quad + (a_m + b_m)u^m + a_{m+1}u^{m+1} + \cdots + a_nu^n.\end{aligned}$$

0 也是一个多项式，而 $\sum_{i=0}^{n} a_iu^i$ 的負元素是多項式 $\sum_{i=0}^{n} (-a_i)u^i$. 最后，因为 $(a_iu^i)(b_ju^j) = a_ib_ju^{i+j}$，故

$$(9)\qquad \begin{aligned}&(a_0+a_1u+a_2u^2+\cdots+a_nu^n)(b_0+b_1u+\cdots+b_mu^m)\\ &= p_0 + p_1u + \cdots + p_{n+m}u^{n+m},\end{aligned}$$

这里

$$(10).\qquad p_i = \sum_{j=0}^{i} a_jb_{i-j} \equiv \sum_{j+k=i} a_jb_k.$$

故多項式全部成为 $\mathfrak{B}$ 的一个子环. 这个子环显然含有 $\mathfrak{A}$，并且因为 $\mathfrak{A}$ 含有 1，故 $u = 1u$ 是一个多項式. 于是，由 $\mathfrak{A}$ 及 u 生成的环 $\mathfrak{A}[u]$ 恰好是 u 的多項式的集合，它們的系数属于 $\mathfrak{A}$.

如果元素 u 关于 $\mathfrak{A}$ 是**超越的**，亦即如果多項式关系

$$d_0 + d_1u + d_2u^2 + \cdots + d_mu^m = 0,\quad d_i \in \mathfrak{A}$$

只能在所有 $d_i = 0$ 时才成立；这种情形特别簡単. 此时，两个多項式 $\sum_0^n a_iu^i$ 及 $\sum_0^m b_ju^j$ 要相等只有对应系数 a_i 与 b_i 相等. 这因为，如果 $n \geqslant m$，并且 $\sum a_iu^i = \sum b_ju^j$，则

$$\begin{aligned}&(a_0 - b_0) + (a_1 - b_1)u + \cdots + (a_m - b_m)u^m\\ &\quad + a_{m+1}u^{m+1} + \cdots + a_nu^n = 0;\end{aligned}$$

于是，$a_j = b_j$，$(j = 1, 2, \cdots, m)$ 而 $a_{m+1} = \cdots = a_n = 0$.

如果 u 不是超越元素，则說：u 关于子环 $\mathfrak{A}$ 是**代数元素**. 要决定多項式环的結构，主要在于有形状如 $\mathfrak{A}[x]$ 的可用的环，这里 x 是超越元素. 在用超越元素作的多項式扩张里，多項式(7)决定唯一的序列$(a_0, a_1, \cdots)$，它附带有 i 是充分大时 $a_i = 0$ 的性質. 故要作 $\mathfrak{A}[x]$，自然选定下面的步驟.

令 $\mathfrak{A}$ 是給定的一个带恆等元素环，幷令 $\mathfrak{B}$ 是无限序列

$$(a_0, a_1, a_2, \cdots)$$

的全部. 这序列里只有有限个非零項 a_i. $\mathfrak{B}$ 里元素作为相等，必須而且只須对于所有 i, $a_i = b_i$. $\mathfrak{B}$ 里的加法定义为

(11)
$$(a_0, a_1, a_2, \cdots) + (b_0, b_1, b_2, \cdots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \cdots).$$

因为序列里从某一項起都是零，故右端所得的和属于 $\mathfrak{B}$. $\mathfrak{B}$ 关于这样加法显然成交換羣. $0 = (0, 0, \cdots)$, 幷且 $-(a_0, a_1, \cdots) = (-a_0, -a_1, \cdots)$. $\mathfrak{B}$ 里的乘法定义为

(12)
$$(a_0, a_1, a_2, \cdots)(b_0, b_1, b_2, \cdots) = (p_0, p_1, p_2, \cdots),$$

这里的 p_i 由 (10) 給出. 如果 $i>n$ 时取 $a_i=0$; $j>m$ 时取 $b_j=0$. 則 $k > m + n$ 时, $p_k = 0$. 故 (12) 的积还是 $\mathfrak{B}$ 里一个元素.

令 $a = (a_0, a_1, \cdots)$, $b = (b_0, b_1, \cdots)$ 及 $c = (c_0, c_1, \cdots)$, 則 $(ab)c$ 里下标为 i 的項是

$$\sum_{m+l=i} \left(\sum_{j+k=m} a_j b_k \right) c_l = \sum_{j+k+l=i} a_j b_k c_l.$$

同理, $a(bc)$ 的对应項是

$$\sum_{m+j=i} a_j \left(\sum_{k+l=m} b_k c_l \right) = \sum_{j+k+l=i} a_j b_k c_l.$$

故 $(ab)c = a(bc)$. 仿此可驗証分配律成立. 于是, $\mathfrak{B}$, +, · 是一个环.

由元素

$$a' = (a, 0, 0, \cdots)$$

組成的子集合 $\mathfrak{A}'$ 是 $\mathfrak{B}$ 的一个子环，在对应 $a \to a'$ 下与 $\mathfrak{A}$ 同构. 故 $\mathfrak{A}$ 被嵌入于 $\mathfrak{B}$ 內. $\mathfrak{A}'$ 的元素 $1' = (1, 0, \cdots)$ 在 $\mathfrak{B}$ 里具有恆等元素的作用. 今令 x 表元素 $(0, 1, 0, 0, \cdots)$, 則

$$x^k = (0, 0, \cdots, 0, \overset{(k+1)}{1}, 0, \cdots),$$

幷且

$$a' x^k = (0, 0, \cdots, 0, \overset{(k+1)}{a}, 0, \cdots) = x^k a'.$$

故 x 与每个 $a' \in \mathfrak{A}'$ 可交换，并且一般元素 $(a_0, a_1, \cdots, a_n, 0, 0, \cdots)$ 可写成

(13) $$a'_0 + a'_1x + a'_2x^2 + \cdots + a'_nx^n.$$

于是，$\mathfrak{B} = \mathfrak{A}'[x]$. 如果 (13) 等于 0，則 $(a_0, a_1, \cdots) = 0$；于是，所有 $a_i = 0$，从而所有 $a'_i = 0$. 这指出 x 关于 $\mathfrak{A}'$ 是超越元素.

所以，我們可以同构环 $\mathfrak{A}'$ 代替环 $\mathfrak{A}$，并且就把前者写作 $\mathfrak{A}$. 此外还把元素 a' 写作 a. 因此，就得所求的 $\mathfrak{B} = \mathfrak{A}[x]$，并且 x 关于 $\mathfrak{A}$ 是超越的.

习 題 39

1. 令 $\mathfrak{B}^*$ 是序列 $(a_0, a_1, a_2, \cdots)$ 的全部，$a_i \in \mathfrak{A}$. 关于等式、加法及乘法的定义与在环 $\mathfrak{B}$ 里的定义相同. 求証：$\mathfrak{B}^*$ 是一个环. 这个环叫做 $\mathfrak{A}$ 上形式冪級数环，此后記作 $\mathfrak{A}\langle x\rangle$.

2. 令 S 是任一个半羣，并令 $\mathfrak{A}$ 是任一个环. 令 $a(s)$ 是定义在 S 上的函数，它的值 $\in \mathfrak{A}$，且除有限个 s 外，$a(s) = 0$. 令 $\mathfrak{B}$ 是这样函数 $a(s)$ 的集合. 在 $\mathfrak{B}$ 里加法及乘法定义为

$$(a+b)(s) = a(s) + b(s),$$
$$(ab)(s) = \sum_{tu=s} a(t)b(u).$$

驗証：$\mathfrak{B}$ 是一个环，叫做半羣环.

3. 驗証：由非負整数与加法合成組織的半羣所决定的半羣环是上面所作的环 $\mathfrak{A}[x]$.

5. 多項式环的結构 令 x 是基环 $\mathfrak{A}_1$ 上的超越元素，而 $\mathfrak{A}_1[x]$ 是 x 的多項式环，并令 $\mathfrak{A}_2[u]$ 是一个任意多項式环，且 $\mathfrak{A}_2$ 是 $\mathfrak{A}_1$ 的一个同态象. 与前此一样，我們假定这两个环都含有恆等元素，并且 x, u 各与它們的系数环可交换. 令 σ 是 $\mathfrak{A}_1$ 到 $\mathfrak{A}_2$ 上的一个确定同态. 今来証明：这个同态必有而且只有一种方法扩张为 $\mathfrak{A}_1[x]$ 到 $\mathfrak{A}_2[u]$ 上的一个同态，而把 x 映到 u.

因为 x 是超越的，故 $\mathfrak{A}_1[x]$ 的一个元素必有而且只有一种方法写成形状

$$a_0 + a_1x + \cdots + a_nx^n, \quad a_i \in \mathfrak{A}_1.$$

我們用 $f(x)$ 表示它，并定义

$$f^\sigma(u) = a_0^\sigma + a_1^\sigma u + \cdots + a_n^\sigma u^n, \quad a_i^\sigma \in \mathfrak{A}_2.$$

显然 $f(x) \to f^\sigma(u)$ 定义了 $\mathfrak{A}_1[x]$ 到 $\mathfrak{A}_2[u]$ 上的一个单值映照. 如

果 $g(x)=\sum b_i x^i$，则 $f(x)+g(x)=\sum(a_i+b_i)x^i$，而且这个元素映到

$$\sum(a_i+b_i)^\sigma u^i=\sum(a_i^\sigma+b_i^\sigma)u^i$$
$$=\sum a_i^\sigma u^i+\sum b_i^\sigma u^i.$$

再则，

$$f(x)g(x)$$
$$=a_0b_0+(a_0b_1+a_1b_0)x+(a_0b_2+a_1b_1+a_2b_0)x^2+\cdots$$
$$\rightarrow(a_0b_0)^\sigma+(a_0b_1+a_1b_0)^\sigma u+(a_0b_2+a_1b_1+a_2b_0)^\sigma u^2+\cdots$$
$$=a_0^\sigma b_0^\sigma+(a_0^\sigma b_1^\sigma+a_1^\sigma b_0^\sigma)u+(a_0^\sigma b_2^\sigma+a_1^\sigma b_1^\sigma+a_2^\sigma b_0^\sigma)u^2+\cdots$$
$$=(\sum a_i^\sigma u^i)(\sum b_i^\sigma u^i).$$

故这映照是一个同态．如果 $a\in\mathfrak{A}_1$，显然，在新的映照中仍有 $a\rightarrow a^\sigma$，而且 $x\rightarrow u$，因此，这映照满足我們所有的要求．

今令 Σ 是 $\mathfrak{A}_1[x]$ 到 $\mathfrak{A}_2[u]$ 上的任一个同态，把 x 映到 u；且在 $\mathfrak{A}_1$ 上与 σ 的效果一致．则

$$(\sum a_i x^i)^\Sigma=\sum a_i^\Sigma u^i=\sum a_i^\sigma u^i$$

故 Σ 与曾經定义的映照重合．这就証明了扩张的唯一性．于是，得下面重要的同态定理．

定理 4. 令 $\mathfrak{A}_1[x]$ 是超越元素 x 的多项式环，並令 $\mathfrak{A}_2[u]$ 是任意元素 u 的多项式环． 設 σ 是 $\mathfrak{A}_1$ 到 $\mathfrak{A}_2$ 上的一个同态，则 σ 必有而且只有一种方法扩張成 $\mathfrak{A}_1[x]$ 到 $\mathfrak{A}_2[u]$ 上的一个同态 Σ，它把 x 映到 u．

如果 $\mathfrak{A}=\mathfrak{A}_1=\mathfrak{A}_2$，而 σ 是恆等映照，则这个定理指出：对于任意的 u，$\mathfrak{A}[u]$ 是超越元素 x 的多项式环 $\mathfrak{A}[x]$ 的一个同态象．故由同态的基本定理知：$\mathfrak{A}[u]\cong\mathfrak{A}[x]/\mathfrak{K}$ 这里同态核 $\mathfrak{K}$ 是 $\mathfrak{A}[x]$ 里一个理想．因为同态 Σ 在 $\mathfrak{A}$ 里是恆等映照，显然 $\mathfrak{A}\cap\mathfrak{K}=0$．今假定 u 也是超越元素，如果 $f(x)^\Sigma=0$，则必有 $f(u)=0$；故 $f(x)=0$．这指出 $\mathfrak{K}=0$．于是，Σ 是一个同构．故得下面的定理．

定理 5. 如果 x 及 y 都是 $\mathfrak{A}$ 上超越元素，则 $\mathfrak{A}[x]$ 与 $\mathfrak{A}[y]$ 是同構的． 形狀如 $\mathfrak{A}[u]$ 的任一个环必同構于差环 $\mathfrak{A}[x]/\mathfrak{K}$，这里 x 是超越元素，而 $\mathfrak{K}$ 是 $\mathfrak{A}[x]$ 里使 $\mathfrak{K}\cap\mathfrak{A}=0$ 的一个理想．

6. 环 $\mathfrak{A}[x]$ 的性质 由現在起，x 将表示 $\mathfrak{A}$ 上一个超越元素．如果 $f(x)$ 是 $\mathfrak{A}[x]$ 里一个非零多項式，則可写成

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$

这里 $a_n \neq 0$，叫做 $f(x)$ 的首項系数，并叫 n 做 $f(x)$ 的次．如果 $f(x) = 0$，則說它的次是 $-\infty$，并采用通常的規定：$-\infty - \infty = -\infty$，$-\infty + n = -\infty$．

如果 a_n 不是 $\mathfrak{A}$ 里一个左零因子，而 $g(x) = b_0 + b_1x + \cdots + b_mx^m$，$b_m \neq 0$，則

$$f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{n+m}.$$

因为 $a_nb_m \neq 0$，故 $f(x)g(x) \neq 0$，而且这个多項式是 $m + n$ 次．如果 a_n 不是一个右零因子，类似結果对于 $g(x)f(x)$ 也成立．特別是，如果 $\mathfrak{A}$ 是一个整区，則 $\mathfrak{A}[x]$ 也是一个整区．再則，設以 $\deg f(x)$ 表 $f(x)$ 的次数，則对于所有 $f(x)$ 及 $g(x)$，公式

(14) $$\deg f(x)g(x) = \deg f(x) + \deg g(x)$$

成立．这在 $f \neq 0$ 及 $g \neq 0$ 的情形上面已經証过．如果 $f = 0$ 或者 $g = 0$，則由关于 $-\infty$ 的規定，易知也是成立的．我們还要說出关于次数的下面有用結果：

(15) $$\deg [f(x) + g(x)] \leqslant \max (\deg f(x), \deg g(x)).$$

由次数关系 (14) 可决定 $\mathfrak{A}[x]$ 里单位元素．这因为，如果 $f(x)g(x) = 1$，則 $\deg f(x) + \deg g(x) = 0$，故 $\deg f(x) = 0 = \deg g(x)$．于是，$f(x) = a \in \mathfrak{A}$，并且 $g(x) = b \in \mathfrak{A}$．这証明了：如果 $\mathfrak{A}$ 是一个整区，則 $\mathfrak{A}[x]$ 里仅有的单位元素是 $\mathfrak{A}$ 里的单位元素．例如，設 I 是整数环，則 $I[x]$ 里仅有的单位元素是整数 ± 1．又若 $\mathfrak{F}$ 是一个域，則 $\mathfrak{F}[x]$ 的单位元素是 $\mathfrak{F}$ 的非零元素．

再就 $\mathfrak{A}$ 为一个任意整区来考究．我們試图在 $\mathfrak{A}[x]$ 里建立除法算法．令 $g(x) = b_0 + b_1x + \cdots + b_mx^m$ 是任一个非零多項式，它的首項系数 b_m 是一个单位元素．設 $f(x)$ 是任意多項式，我們将驗証：有多項式 $q_1(x)$ 及 $r_1(x)$ 存在，使 $\deg r_1(x) < \deg g(x)$，并且

(16) $$f(x) = q_1(x)g(x) + r_1(x).$$

如果 $\deg f(x) < \deg g(x)$，則可写成 $f(x) = 0 \cdot g(x) + f(x)$ 以获得所求的表示。今設 $f(x) = a_0 + a_1x + \cdots + a_nx^n$ 的次数 $n \geqslant m$。我們可假定这結果对于次数 $<n$ 的多項式 f 成立，而使用归納法。令

$$f(x) - a_n b_m^{-1} x^{n-m} g(x) = f_1(x).$$

則 $f(x)$ 与 $a_n b_m^{-1} x^{n-m} g(x)$ 里最大次数的項都是 a_nx^n，可以相消。故 $\deg f_1(x) < \deg f(x)$。因此可設有一个 $q^*(x)$ 及次数小于 m 的一个 $r_1(x)$ 存在，使

$$f_1(x) = q^*(x)g(x) + r_1(x).$$

于是，

$$\begin{aligned} f(x) &= a_n b_m^{-1} x^{n-m} g(x) + q^*(x)g(x) + r_1(x) \\ &= q_1(x)g(x) + r_1(x), \end{aligned}$$

这里 $q_1(x) = a_n b_m^{-1} x^{n-m} + q^*(x)$，并且 $\deg r_1(x) < \deg g(x)$。

"右商" $q_1(x)$ 及"右余項" $r_1(x)$ 是唯一的。这因为，假設

$$f(x) = q_2(x)g(x) + r_2(x), \quad \deg r_2(x) < \deg g(x),$$

則

$$[q_1(x) - q_2(x)]g(x) = r_2(x) - r_1(x).$$

由于右端的次数 $< m$，而左端的次数是 $-\infty$ 或者 $\geqslant m$，所以公共值必須是 $-\infty$；从而 $r_2(x) - r_1(x) = 0$，并且 $q_1(x) - q_2(x) = 0$。

同样可証：使

$$f(x) = g(x)q_2(x) + r_2(x)$$

的"左商" $q_2(x)$ 及次数 $< \deg g(x)$ 的"左余項" $r_2(x)$ 的存在及唯一性。

今就 $g(x) = x - c$，$c \in \mathfrak{A}$ 这一情形来考究。要获得关于以 $x - c$ 除的余項公式可用下面恆等式：

$$(17) \qquad \begin{aligned} x^k - c^k &= (x^{k-1} + cx^{k-2} + c^2x^{k-3} + \cdots + c^{k-1})(x - c) \\ &= (x - c)(x^{k-1} + cx^{k-2} + c^2x^{k-3} + \cdots + c^{k-1}), \\ &\qquad (k = 0, 1, 2, \cdots). \end{aligned}$$

这里要知道：如果 $k = 0$，則因子 $\sum c^i x^{k-i-1} = 0$。設以 a_k 左乘 (17)，并对于 k 求和，得

$$f(x) - f_R(c) = q_1(x)(x - c),$$
这里 $q_1(x) = \sum a_k(x^{k-1} + cx^{k-2} + \cdots + c^{k-1})$, 并且

(18) $$f_R(c) = a_0 + a_1c + a_2c^2 + \cdots + a_nc^n.$$

故 $f(x) = q_1(x)(x - c) + f_R(c)$, 而 $f_R(c)$ 是右余項. 仿此,使用(17)的后一形式,則可証得:以 $x - c$ 除得的左余項是

(19) $$f_L(c) = a_0 + ca_1 + c^2a_2 + \cdots + c^na_n.$$

由这些結果立得:

因子定理. 多項式 $(x - c)$ 是 $f(x)$ 的右(左)因子必須而且只須 c 是一个右(左)根,亦即 $f_R(c) = 0(f_L(c) = 0)$.

如果 $\mathfrak{A}$ 是交換整区,則在上面討論中,当然可把"左"及"右"字删去. 如果 $\mathfrak{A} = \mathfrak{F}$ 是一个域,則除法算法可使用于任意两个多項式 $f(x)$, $g(x) \neq 0$. 这个事实可用以証以下重要的定理.

定理 6. 如果 $\mathfrak{F}$ 是一个域,則 $\mathfrak{F}[x]$ 里每个理想都是主理想.

証 令 $\mathfrak{B}$ 是 $\mathfrak{F}[x]$ 里一个理想. 如果 $\mathfrak{B} = 0$,則理想仅由 0 构成;于是,$\mathfrak{B} = (0)$ 是由 0 生成的主理想. 故假定 $\mathfrak{B} \neq 0$. 令 $g(x)$ 是 $\mathfrak{B}$ 里有最小次数的一个非零多項式. 如果 $f(x)$ 是 $\mathfrak{B}$ 的任一个元素,記 $f(x) = g(x)q(x) + r(x)$, 这里 $\deg r(x) < \deg g(x)$,則 $r(x) = f(x) - g(x)q(x) \in \mathfrak{B}$.但因为它的次数小于 $g(x)$ 的次数,故 $r(x) = 0$. 于是, $f(x) = g(x)q(x)$ 是属于主理想 $(g(x))$. 故 $\mathfrak{B} \subseteq (g(x))$. 但 $g(x) \in \mathfrak{B}$,故又有$(g(x)) \subseteq \mathfrak{B}$.于是,$\mathfrak{B} = (g(x))$.

这定理使我們对于域可得出比定理 5 更尖銳的形式如次:

系 1. 如果 $\mathfrak{F}$ 是一个域, 則任一个多項式环

$$\mathfrak{F}[u] \cong \mathfrak{F}[x]/(g(x)),$$

这里 $g(x) = 0$, 或者 $g(x)$ 是一个多項式, 其次數为正整數.

因为,如果 $g(x)$ 是一个 0 次非零多項式,則可推得 $(g(x)) = \mathfrak{F}[x]$,故这情形的可能性要除外.

习 題 40

1. 如果 $f(x) = a_0 + a_1x + \cdots + a_nx^n$, 定义 $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$. 求証: 通常的法則

$$(f + g)' = f' + g', \quad (cf)' = cf', \quad c \in \mathfrak{A},$$

$$(fg)' = fg' + f'g.$$

2. 求証：李卜尼兹 (Leibniz) 定理

$$(fg)^{(k)} = \sum_0^k \binom{k}{i} f^{(i)} g^{(k-i)},$$

这里 $f^{(i)} = f^{(i-1)'}, f^{(0)} = f$.

7. 域的簡单扩张 本章所启发的方法可用以作任一个給定域 $\mathfrak{F}$ 的域扩张. 我們将要知道，任一个这样扩张可由作一系列的两种类型的簡单扩张而获得.

簡单超越扩张. 对于給定域 $\mathfrak{F}$，先作多項式环 $\mathfrak{F}[x]$，这里 x 是超越元素. 我們知道，$\mathfrak{F}[x]$ 是一个整区，而不是一个域. 但我們能把它嵌入于它的分式域里. 这分式域記作 $\mathfrak{F}(x)$，它的元素叫做基域 $\mathfrak{F}$ 上 x 的有理式(有理函数). 这些元素的形状为 $f(x)/g(x)$，这里 $f(x)$ 及 $g(x)$ 都是多項式，并且 $g(x) \neq 0$. 通用的各計算法則是成立的.

簡单代数扩张. 域的这种扩张方法始創于柯齐 (Cauchy) 把复数域 C 定义成实数域 R 的一种扩张. 按柯齐的方法，作出差环 $C = R[x]/(x^2+1)$，这里 (x^2+1) 是 x^2+1 的倍数組成的主理想. 我們可証：C 是 R 的一种域扩张，它含有方程 $x^2+1=0$ 的一个根. 克伦內克 (Kronecker) 推广柯齐的方法，使用于任一个域 $\mathfrak{F}$ 与任一个多項式 $f(x) \in \mathfrak{F}[x]$；$f(x)$ 在这个整区里是不可約(素)多項式. $f(x)$ 是不可約的意思是說：$f(x)$ 不能分解为两个正次数的多項式的积，这里还假定 $\deg f(x) > 0$.

今就前面提出的情形作差环 $\mathfrak{E} = \mathfrak{F}[x]/(f(x))$，这里 $(f(x))$ 照惯例表示由 $f(x)$ 生成的主理想. 环 $\mathfrak{E}$ 拥有恆等元素 $\bar{1} = 1 + (f(x))$，并且因为 $f(x)$ 的次数是正数，故 $\bar{1} \neq 0$. 今考究任一个陪集 $\overline{g(x)} = g(x) + (f(x)) \neq 0$. 令 $\mathfrak{B}$ 是形状如 $u(x)g(x) + v(x)f(x)$ 的多項式的全部，这里 $u(x)$ 及 $v(x)$ 是 $\mathfrak{F}[x]$ 里任意多項式. 显然，$\mathfrak{B}$ 是 $\mathfrak{F}[x]$ 里一个理想，故 $\mathfrak{B} = (d(x))$. 因为 $f(x) = 0 \cdot g(x) + 1 \cdot f(x) \in \mathfrak{B}$，故 $f(x) = d(x)f_1(x)$. 于是，$d(x)$ 或者是 $\mathfrak{F}$ 的一个非零元素，或者是 $f(x)$ 的一个倍数(亦即与 $\mathfrak{F}$ 的元素之积). 另一方面，$g(x) \in \mathfrak{B}$，故 $g(x) = d(x)g_1(x)$. 于是，如果 $d(x)$ 是 $f(x)$

的倍数，则 $g(x)$ 是 $f(x)$ 的一个倍数，这与 $\overline{g(x)} \neq 0$ 的假設矛盾。故知 $d(x) = d$ 是$\mathfrak{F}$的一个非零元素。因为 $d \in \mathfrak{B}$，故这个元素的形状是 $u(x)g(x) + v(x)f(x)$。設乘以 d^{-1}，则得多項式 $a(x)$，$b(x)$，使

$$a(x)f(x) + b(x)g(x) = 1. \tag{20}$$

由关系 (20) 給出 $\overline{a(x)}\ \overline{f(x)} + \overline{b(x)}\ \overline{g(x)} = \bar{1}$。因为 $\overline{f(x)} = 0$，故 $\overline{b(x)}\ \overline{g(x)} = \bar{1}$。所以，$\mathfrak{E}$ 的任一个非零元素有一个逆元素。因为 $\mathfrak{E}$ 是可交换的，故 $\mathfrak{E}$ 是一个域。

其次要指出：$\mathfrak{E}$ 是 $\mathfrak{F}$ 的一个扩张。試考究 $\mathfrak{F}[x]$ 到 $\mathfrak{E}$ 上的自然同态 $g(x) \to \overline{g(x)}$。这个映照导出 $\mathfrak{F}$ 到 $\mathfrak{E}$ 的一个子环 $\bar{\mathfrak{F}}$ 上的一个同态。象集合 $\bar{\mathfrak{F}}$ 是陪集 $\bar{a} = a + (f(x))$ 的全部，这里 $a \in \mathfrak{F}$，故它包括 $\bar{1} \neq 0$ 在内。另一方面，$\mathfrak{F}$ 是一个域，故它的同态象或者是 0，或者与 $\mathfrak{F}$ 是同构的。于是，$\bar{\mathfrak{F}} \cong \mathfrak{F}$。这样一来，$\mathfrak{F}$ 就被嵌入于 $\mathfrak{E}$ 内。我們照惯例把 $\bar{\mathfrak{F}}$ 与 $\mathfrak{F}$ 恆等起来，并以 a 表陪集 $\bar{a}$。

末了，我們指出：$\mathfrak{E} = \mathfrak{F}[\bar{x}]$ 并且 $\bar{x}$ 是适合方程 $f(\bar{x}) = 0$ 的一个代数元素。首先，如果 $g(x)$ 是任一个多項式，则 $\overline{g(x)} = g(\bar{x})$ 是 $\bar{x}$ 的一个多項式，其系数 $\in \mathfrak{F}$。事实上，容易知道，$\mathfrak{E}$ 的任一个元素可表作 $\bar{x}$ 的一个多項式，其次数 $< \deg f(x)$。这因为，$g(x)$ 可写作 $g(x) = f(x)q(x) + r(x)$，这里 $\deg r(x) < \deg f(x)$。故 $\overline{g(x)} = \overline{r(x)} = r(\bar{x})$。因为 $0 = \overline{f(x)} = f(\bar{x})$，故 $\bar{x}$ 是方程 $f(x) = 0$的一个根。

如果 $f(x)$ 是可約多項式，则差环 $\mathfrak{E} = \mathfrak{F}[x]/(f(x))$ 还是可以作的。設 $f(x) = f_1(x)f_2(x)$，这里 $\deg f_i(x) > 0$，则 $\overline{f_i(x)} \neq 0$，且 $\overline{f_i(x)} \in \mathfrak{E}$。但 $\overline{f_1(x)}\ \overline{f_2(x)} = \overline{f(x)} = 0$。故此时得出带有非零的零因子的一个环。无論如何，$\mathfrak{E}$ 显然是可交换的，且拥有恆等元素。

习 題 41

1. 令 $\mathfrak{E} = R_0[x]/(x^3 + 3x - 2)$。求把 $\mathfrak{E}$ 的元素

(a) $$(2\bar{x}^2 + \bar{x} - 3)(3\bar{x}^2 - 4\bar{x} + 1),$$

(b) $$(2\bar{x}^2 + 4\bar{x} - 5)^{-1}$$

列成 x 的多项式,其次数 <3.

2. 如果 $f(x)$ 有一个平方因子 $(f(x)=[f_1(x)]^2f_2(x),\ \deg f_1(x)>0)$, 验証: $\mathfrak{E}=\mathfrak{F}[x]/(f(x))$ 含有非零无势元素.

8. 任意域的結构 要分析任一个域 $\mathfrak{F}$ 的結构, 先考察 $\mathfrak{F}$ 的最小子域 $\mathfrak{P}$, 这样域叫做 $\mathfrak{F}$ 的素域. 我們知道, $\mathfrak{F}$ 的任意个子域的交还是一个子域,故素域可定义为 $\mathfrak{F}$ 的所有子域的交.

我們知道, $\mathfrak{P}$ 含有 1; 故 $\mathfrak{P}$ 含有由 1 生成的子环 $[[1]]$. 但我們知道, 由 1 生成的一个环必与 I 或 $I/(m)$, $m>0$ 是同构的(第二章 § 9). 如果与 $I/(m)$ 是同构的,则 $m=p$ 是一个素数. 这因为, 否则 $I/(m)$ 有零因子 $\neq 0$,結果将使 $[[1]]$ 有零因子 $\neq 0$, 但这对于一个域来說显然是不可能的. 故有下面两种可能性:

I $$[[1]]\cong I,$$

II $$[[1]]\cong I/(p),\quad p\text{ 是素数.}$$

如果 I 成立, 则 $[[1]]$ 是一个整区, 但不是一个域. 故要获得素域必須取形状如 $(m1)(n1)^{-1}$ 的元素的全部, 这里 $m,n\in I$, 并且 $n\neq 0$. 故 $\mathfrak{P}$ 显然与有理数域是同构的. 如果 II 成立,则因 $I/(p)$ 是一个域, 故 $[[1]]$ 是一个域. 在情形 I 下, $\mathfrak{F}$ 显然有特征数 0, 而在情形 II 下有特征数 p.

次設 $\mathfrak{F}_0$ 是 $\mathfrak{F}$ 的任一个子域. 我們今来决定: 由 $\mathfrak{F}_0$ 及附加 $\mathfrak{F}$ 的元素 θ (可能 $\in\mathfrak{F}_0$)所生成的子域 $\mathfrak{F}_0(\theta)$ 的結构. 先考究由 $\mathfrak{F}_0$ 及 θ 生成的子环 $\mathfrak{F}_0[\theta]$. 我們知道(§ 6 系 1): $\mathfrak{F}_0[\theta]\cong\mathfrak{F}_0[x]/(f(x))$, 这里 $f(x)=0$ 或者 $f(x)$ 有正次数. 理想 $(f(x))$ 是同态 $g(x)\to g(\theta)$ 的核. 今設 $f(x)$ 是可約的, 则 $\mathfrak{E}=\mathfrak{F}_0[x]/(f(x))$ 不是一个整区,故这个可能性要除外;于是,有下面的两种可能性:

I $$\mathfrak{F}_0[\theta]\cong\mathfrak{F}_0[x],$$

II $$\mathfrak{F}_0[\theta]\cong\mathfrak{F}_0[x]/(f(x)),\quad f(x)\text{ 是不可約的.}$$

如果 I 成立, 则 θ 是超越元素, 并且 $\mathfrak{F}_0(\theta)$ 与 x 的有理式域 $\mathfrak{F}_0(x)$ 是同构的. 如果 II 成立, 则 $f(\theta)=0$, 故 θ 是代数元素. 此时, 因为 $\mathfrak{F}_0[x]/(f(x))$ 是一个域, 故 $\mathfrak{F}_0[\theta]$ 是一个域. 于是, $\mathfrak{F}_0(\theta)=\mathfrak{F}_0[\theta]$. 故知无論那一种情形, $\mathfrak{F}_0(\theta)$ 实质上必属于前节所討論的

$\mathfrak{F}_0$的簡单扩张的一种.

至此，我們知道：任一个域的素域的特性及任一个子域$\mathfrak{F}_0(\theta)$的特性. 今将指出：任一个域可在素域上接連用簡单(代数或超越)扩张建立起来.对于一个給定域要証明这个結果，需要这个域是良序的[1]. 无論如何，作为下面論点基础的代数观念可由考虑可数情形而完全揭露出来. 所以，我們假定$\mathfrak{F}$为可数的(亦卽为有限的或可数无限的)，并假設$\theta_1, \theta_2, \theta_3, \cdots$是$\mathfrak{F}$的元素的一种編列. 令$\mathfrak{F}_0 = \mathfrak{P}$, $\mathfrak{F}_i = \mathfrak{F}_{i-1}(\theta_i)$，則$\mathfrak{F} = \bigcup \mathfrak{F}_i$，并且每个$\mathfrak{F}_i$是从$\mathfrak{F}_{i-1}$經过簡单超越扩张或簡单代数扩张得出.

9. 域上多項式的根的个数　如果$f(x)$是系数在一个域上的一个多項式，而c_1是$f(x) = 0$的一个根，則$f(x) = (x-c_1)f_1(x)$. 今設$c_1, c_2, \cdots, c_m$是$f(x) = 0$的不同的根. 以c_2代入$f(x) = (x - c_1)f_1(x)$（亦卽使用同态$g(x) \to g(c_2)$)，得

$$0 = f(c_2) = (c_2 - c_1)f_1(c_2).$$

因为$c_2 \neq c_1$，故$f_1(c_2) = 0$. 于是，$f_1(x) = (x - c_2)f_2(x)$，并且$f(x) = (x - c_1)(x - c_2)f_2(x)$. 这样継續下去，可証：

$$f(x) = (x - c_1)(x - c_2)\cdots(x - c_m)f_m(x).$$

由此显然可推得：$f(x)$的次数$n \geqslant m$. 这証明了下面的定理.

定理 7. 如果$\mathfrak{F}$是一个域，並且$f(x)$是系數屬于$\mathfrak{F}$的n ($\geqslant 0$)次多項式，則$f(x)$在$\mathfrak{F}$里至多有n个不同的根.

习　題　42

1. 設$a_n \not\equiv 0 \pmod{p}$，則同余式$a_0 + a_1x + \cdots + a_nx^n \equiv 0 \pmod{p}$在$I$里至多只有$n$个非同余解.
2. 如果$\mathfrak{F}$是含有q个元素a_i的一个有限域，求証：在$\mathfrak{F}[x]$里，
$$h(x) = x^q - x = (x - a_1)(x - a_2)\cdots(x - a_q).$$
3. 如果p是素数，求証：$(p - 1)! \equiv -1 \pmod{p}$.这叫做威尔孙(Wilson)定理.
4. 驗証：多項式$x^3 - x$在$I/(6)$里有6个根.
5. 驗証：多項式$x^2 + 1$在实四維数环Q里有无限个根.

10. 多变元多項式　再令$\mathfrak{B}$是一个带恆等元素环，并令$\mathfrak{A}$是

1) 关于良序的討論，参看范德威尔登(van der Waerden)的"近世代数"(Moderne Algebra)卷1，初版，第八章. ——著者注.

含有1的任一个子环. 設 $u_1, u_2, \cdots, u_r$ 是 $\mathfrak{B}$ 的元素，它們可以交换. 而且也可与各个 $a\in\mathfrak{A}$ 交换. 令 $\mathfrak{A}[u_1, u_2, \cdots, u_r]$ 表由 $\mathfrak{A}$ 及 u_i 生成的子环，并記 $(((\mathfrak{A}[u_1])[u_2])\cdots)[u_r]$ 为 $\mathfrak{A}[u_1][u_2]\cdots[u_r]$，则我們可証

(21) $$\mathfrak{A}[u_1, u_2, \cdots, u_r] = \mathfrak{A}[u_1][u_2]\cdots[u_r].$$

这在 $r=1$ 时显然成立. 假定它对于 $s-1$ 成立，而考究 $\mathfrak{A}[u_1, u_2, \cdots, u_s]$. 这个环含有 $\mathfrak{A}[u_1, u_2, \cdots, u_{s-1}]$ 及元素 u_s，故含有 $\mathfrak{A}[u_1, \cdots, u_{s-1}][u_s]$. 反过来 $\mathfrak{A}[u_1, \cdots, u_{s-1}][u_s]$ 是含有 $u_1, u_2, \cdots, u_s$ 的一个子环. 故它含有 $\mathfrak{A}[u_1, \cdots, u_s]$. 于是，由归納法假設得

$$\begin{aligned}\mathfrak{A}[u_1, \cdots, u_s] &= \mathfrak{A}[u_1, \cdots, u_{s-1}][u_s]\\ &= \mathfrak{A}[u_1]\cdots[u_{s-1}][u_s].\end{aligned}$$

由(21)或直接地可見 $\mathfrak{A}[u_1,u_2,\cdots,u_r]$ 是 $u_1, u_2, \cdots, u_r$ 的**多項式**

$$\sum a_{i_1 i_2\cdots i_r} u_1^{i_1} u_2^{i_2}\cdots u_r^{i_r}$$

的全体，它們**系数** $a_{i_1 i_2\cdots i_r}$ 属于 $\mathfrak{A}$. 如果形状为

(22) $$\sum d_{i_1 i_2\cdots i_r} u_1^{i_1} u_2^{i_2}\cdots u_r^{i_r} = 0,\quad d_{i_1 i_2\cdots i_r}\in\mathfrak{A}$$

的关系只在所有 d 等于0时才能成立，则說 $u_1, u_2, \cdots, u_r$ 是 $\mathfrak{A}$ **上代数无关元素**. 这可認为是超越元素概念的推广. 因为 u 是可交换的，显然这个条件与元素 $u_1, u_2, \cdots, u_r$ 的次序无关. 又由定义显見：u_1 是 $\mathfrak{A}$ 上代数无关元素必須而且只須它是超越元素. 今来証明下面更一般的結果：

引理. $u_1, u_2, \cdots, u_r$ 是 $\mathfrak{A}$ 上代数无关元素必須而且只須每个 $u_k (k=1, 2, \cdots, r)$ 是 $\mathfrak{A}[u_1, u_2, \cdots, u_{k-1}]$ 上超越元素.

証 設每个 $u_k (k=1, 2, \cdots, r)$ 是 $\mathfrak{A}[u_1, \cdots, u_{k-1}]$ 上超越元素，并設(22)成立. 把这个关系写成

(23) $$D_0 + D_1 u_r + D_2 u_r^2 + \cdots + D_m u_r^m = 0,$$

这里 $D_i = \sum d_{i_1 i_2\cdots i_{r-1} i} u_1^{i_1} u_2^{i_2}\cdots u_{r-1}^{i_{r-1}}$，则每个 $D_i = 0$. 使用归納法，我們可假定由此能推得 $d_{i_1 i_2\cdots i_{r-1} i} = 0$ 对于所有 $i_1, i_2, \cdots$ 成立. 故 u_i 是代数无关的. 反过来，設 $u_1, u_2, \cdots, u_r$ 是代数无关

元素的集合，并設有形状如 $\sum D_i u_k^i = 0$ 的一个关系，这里 $D_i \in \mathfrak{A}[u_1, u_2, \cdots, u_{k-1}]$，則可写 $D_i = \sum d_{i_1 i_2 \cdots i_{k-1} i} u_1^{i_1} u_2^{i_2} \cdots u_{k-1}^{i_{k-1}}$，并得出 $\sum d_{i_1 i_2 \cdots i_{k-1} i} u_1^{i_1} u_2^{i_2} \cdots u_{k-1}^{i_{k-1}} u_k^i = 0$. 于是，对于所有 $i_1, i_2, \cdots, i$ 得 $d_{i_1 i_2 \cdots i_{k-1} i} = 0$，并且对于所有 i，$D_i = 0$. 故 u_k 是 $\mathfrak{A}[u_1, u_2, \cdots, u_{k-1}]$ 上超越元素.

这个引理使我們对于任一个給定的带恆等元素环 $\mathfrak{A}$ 依归納法作出一个环 $\mathfrak{B} = \mathfrak{A}[x_1, x_2, \cdots, x_r]$，这里 x_i 是 $\mathfrak{A}$ 上代数无关元素. 这因为，我們可接連地作出环 $\mathfrak{A}[x_1]$，$\mathfrak{A}[x_1][x_2]$，$\cdots$，这里每个 x_k 是 $\mathfrak{A}[x_1]\cdots[x_{k-1}] = \mathfrak{A}[x_1, \cdots, x_{k-1}]$ 上超越元素. 故 $\mathfrak{A}[x_1]\cdots[x_r] = \mathfrak{A}[x_1, \cdots, x_r]$ 显然是所求形状的环.

如果 x_i 是 $\mathfrak{A}$ 上代数无关元素，而 $y_i (i = 1, 2, \cdots, r)$ 也是 $\mathfrak{A}$ 上代数无关元素，則 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ 与 $\mathfrak{A}[y_1, y_2, \cdots, y_r]$ 是同构的. 这是下面定理的直接結果.

定理 8. 令 $\mathfrak{A}_i (i = 1, 2)$ 是一个帶恆等元素环，並令 $\mathfrak{A}_i[x_{1i}, x_{2i}, \cdots, x_{ri}]$ 是代數无关元素 x_{ji} 的多項式环，則 $\mathfrak{A}_1$ 到 $\mathfrak{A}_2$ 上任一个同态(同構)必有而且只有一种方法扩張为 $\mathfrak{A}_1[x_{11}, x_{21}, \cdots, x_{r1}]$ 到 $\mathfrak{A}_2[x_{12}, x_{22}, \cdots, x_{r2}]$ 上的一个同态(同構)，而把 x_{j1} 映到 $x_{j2} (j = 1, 2, \cdots, r)$.

在 $r = 1$ 的情形，前节中已經証明了. 由归納法即可扩张到任意的 r；詳細論証让讀者来做.

同样的归納法步驟还可得出下面两个結果：(1) 如果 $\mathfrak{A}$ 是一个整区，則 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ 也是一个整区. (2) 如果 $\mathfrak{A}$ 是一个整区，則 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ 的仅有单位元素即是 $\mathfrak{A}$ 里单位元素.

习 題 43

1. 設 x_i 是代数无关元素，驗証：一个环 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ 还可由非負整数 i_j 的 r 維組 $(i_1, i_2, \cdots, i_r)$ 的半羣 S 的 $\mathfrak{A}$ 上半羣环得出，这里合成是

$$(i_1, i_2, \cdots, i_r)(j_1, j_2, \cdots, j_r) = (i_1 + j_1, i_2 + j_2, \cdots, i_r + j_r).$$

***11. 对称多項式**　設 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ 的元素 x_i 是代数无关的. 如果 $x_{1'}, x_{2'}, \cdots, x_{r'}$ 是 $x_1, x_2, \cdots, x_r$ 的任一个置換，显然 $\mathfrak{A}[x_1, x_2, \cdots, x_r] = \mathfrak{A}[x_{1'}, x_{2'}, \cdots, x_{r'}]$. 故由上面定理知，

映照

(24) $$\sum a_{i_1 i_2 \cdots i_r} x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r} \to \sum a_{i_1 i_2 \cdots i_r} x_{1'}^{i_1} x_{2'}^{i_2} \cdots x_{r'}^{i_r}$$

是 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ 的一个自同构. 故 x 的置换

$$\sigma: \begin{pmatrix} x_1 & x_2 & \cdots & x_r \\ x_{1'} & x_{2'} & \cdots & x_{r'} \end{pmatrix}$$

必有而且只有一种方法扩张为 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ 的一个自同构 σ^*, 它在 $\mathfrak{A}$ 里有恆等变換的作用.

今設 A 及 B 是一个环的自同构,則积 AB 也是一个自同构.在特款,如果 σ^* 及 τ^* 是由 S_r 的元素 σ, τ 决定的自同构时,則 $\sigma^*\tau^*$ 是 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ 的一个自同构. 今自同构 $\sigma^*\tau^*$ 及 $(\sigma\tau)^*$ 施于 x_i 的效果与置換 $\sigma\tau$ 施于 x_i 的效果同,并且对于系数环 $\mathfrak{A}$ 的效果是恆等变換. 故由此知 $\sigma^*\tau^* = (\sigma\tau)^*$. 于是,自同构 σ^* 的集合 Σ 是与对称羣 S_r 同构的一个变換羣.

如果一个多項式 $f(x_1, x_2, \cdots, x_r)$ 对于所有 $\sigma^* \in \Sigma$ 都有 $f\sigma^* = f$, 則它叫做 x 的对称多項式. 这种多項式的全体組成 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ 的一个子环 $\mathfrak{S}$. 显然, $\mathfrak{S} \supseteq \mathfrak{A}$. 再則多項式

$$F(x) = (x - x_1)(x - x_2) \cdots (x - x_r)$$

的系数是对称的. 这因为,我們可把 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ 的自同构 σ^* 扩张成 $\mathfrak{A}[x_1, \cdots, x_r, x]$ 的自同构 σ^{**}, 使 $x\sigma^{**} = x$. 扩张 σ^{**} 只把 $F(x)$ 的因子改排过,故把 $F(x)$ 映到它自身. 因此, $F(x)$ 的系数对于 σ^{**} 不变,从而也对于 σ^* 不变. 因为这对于所有 σ 都成立,故 $F(x)$ 的系数都是对称的. 由計算这些系数得

$$F(x) = x^r - p_1 x^{r-1} + p_2 x^{r-2} - \cdots + (-1)^r p_r,$$

这里

(25) $$p_1 = \sum_i x_i, \quad p_2 = \sum_{i<j} x_i x_j, \quad p_3 = \sum_{i<j<k} x_i x_j x_k, \cdots$$
$$p_r = x_1 x_2 \cdots x_r.$$

p_i 我們叫做初等对称多項式,并将証明 $\mathfrak{S} = \mathfrak{A}[p_1, p_2, \cdots, p_r]$,而且 p_i 是 $\mathfrak{A}$ 上代数无关元素.

方程 $\mathfrak{S} = \mathfrak{A}[p_1, p_2, \cdots, p_r]$ 的意义是: 每个对称多項式可

写成初等对称函数 p_i 的一个多项式. 如果一个多项式里所有项 $ax_1^{k_1}x_2^{k_2}\cdots x_r^{k_r}$ 的全次数 $k=k_1+k_2+\cdots+k_r$ 都相同, 这样多项式叫做齐次多项式. 因为一个多项式必有而且只有一个方法写为不同次数的齐次多项式的和, 而且自同构 σ^* 对于次数保持不变. 故若 $f(x_1, x_2, \cdots, x_r)$ 是对称多项式, 显然它的各个齐次部分也是对称的. 故上面結果只要就齐次多项式来証明就可以了.

今設 $f(x_1, x_2, \cdots, x_r)$ 是 m 次齐次对称多项式. 今对于 m 次单项式引入辞典式編列, 亦即对于 $ax_1^{k_1}x_2^{k_2}\cdots x_r^{k_r}$ 及 $bx_1^{l_1}x_2^{l_2}\cdots x_r^{l_r}$, 如果 $k_1=l_1, k_2=l_2, \cdots, k_s=l_s$, 但 $k_{s+1}>l_{s+1}(s\geqslant 0)$, 我們就說 $ax_1^{k_1}x_2^{k_2}\cdots x_r^{k_r}$ 高于 $bx_1^{l_1}x_2^{l_2}\cdots x_r^{l_r}$. 例如, $x_1^2x_2x_3>x_1x_2^3>x_1x_2^2x_3$. 今令 $ax_1^{k_1}x_2^{k_2}\cdots x_r^{k_r}$ 是 f 里的最高項, 则因 f 含有可由 $ax_1^{k_1}x_2^{k_2}\cdots x_r^{k_r}$ 經过 x 的置换而得出所有各項, 故在 f 的最高項里必有 $k_1\geqslant k_2\geqslant\cdots\geqslant k_r$.

今考究齐次对称多项式 $p_1^{d_1}p_2^{d_2}\cdots p_r^{d_r}$ 的最高項. 使用(25)可見这項是

$$x_1^{d_1+d_2+\cdots+d_r}x_2^{d_2+\cdots+d_r}\cdots x_r^{d_r}.$$

故 $ap_1^{k_1-k_2}p_2^{k_2-k_3}\cdots p_r^{k_r}$ 的最高項与 f 的最高項相同. 于是, 齐次对称多项式 $f_1=f-ap_1^{k_1-k_2}p_2^{k_2-k_3}\cdots p_r^{k_r}$ 的最高項必低于 f 的最高項. 将上面方法重复使用于 f_1. 因为低于一个給定項的最高項只有有限个, 故經过有限次使用这方法, 就得出用含 p_i 的多项式来表 f 的一个表示.

今将指出初等对称多项式是代数无关的. 如果含 p_i 的关系里有系数 $\neq 0$. 我們考究 $a_{d_1\cdots d_r}\neq 0$ 的对应指数$(d_1,d_2,\cdots,d_r)$的集合. 引入

$$k_1=d_1+d_2+\cdots+d_r,\quad k_2=d_2+\cdots+d_r,\cdots,$$
$$k_r=d_r.$$

则 $a_{d_1\cdots d_r}p_1^{d_1}p_2^{d_2}\cdots p_r^{d_r}$ 里按辞典式編列的最高項为 $a_{d_1\cdots d_r}x_1^{k_1}x_2^{k_2}\cdots x_r^{k_r}$. 如果 $(d_1', d_2', \cdots, d_r')$ 是使 $a_{d_1'\cdots d_r'}\neq 0$ 的另一个对应指数的集合, 则 $a_{d_1'\cdots d_r'}p_1^{d_1'}p_2^{d_2'}\cdots p_r^{d_r'}$ 的最高項是 $a_{d_1'\cdots d_r'}x_1^{k_1'}x_2^{k_2'}\cdots x_r^{k_r'}$, 这里

$$k_i'=d_i'+d_{i+1}'+\cdots+d_r'\quad (i=1,2,\cdots,r).$$

如果对于所有 i, $k_i = k'_i$，则显然 $d_i = d'_i$. 故含 p 的項不相同，所导出含 x 的最高項也不相同. 如果取項 $a_{d_1\cdots d_r}p_1^{d_1}p_2^{d_2}\cdots p_r^{d_r}$ 使 $x_1^{k_1}x_2^{k_2}\cdots x_r^{k_r}$ 高于其他任一項 $x_1^{k'_1}x_2^{k'_2}\cdots x_r^{k'_r}$，則 $x_1^{k_1}x_2^{k_2}\cdots x_r^{k_r}$ 显然在 p 的关系里只出現一次. 这就得出 x 的一个非当然关系，而与元素 x 是代数无关的假設矛盾. 这証明了下面定理的第二部分.

定理 9. 每个对称多項式可寫成(25)里各个初等对称多項式 p_i 的多項式. 初等对称多項式 $p_1, p_2, \cdots, p_r$ 是 $\mathfrak{A}$ 上代數无关元素. 每个 x_i 是 $\mathfrak{A}[p_1, p_2, \cdots, p_r]$ 上代數元素.

因为

$$F(x_i) = x_i^r - p_1x_i^{r-1} + \cdots + (-1)^r p_r = 0,$$

故定理的最后部分显然为真.

习 题 44

1. 求以初等对称函数表示 $\sum\limits_{i,j,k,\neq} x_i^2x_j^2x_k\ (n \geqslant 5)$.

2. 令 $\Delta = \prod\limits_{i<j}(x_i - x_j)$. 如果 η 是一个对换，驗証：$\Delta\eta^* = -\Delta$. 使用这結果証明：如果 τ 是一个置换它有一个分解是偶(奇)数个对换的积，則 τ 的任一个因子分解成对换的积必含着偶(奇)数个对换.

3. 驗証：Δ^2 是对称的. 就 $r = 3$ 把 Δ^2 用初等对称函数表出.

4. 驗証：对称多項式 $s_k = \Sigma x_i^k$ 适合牛頓 (Newton) 恆等式

$$s_k - p_1s_{k-1} + p_2s_{k-2} - \cdots + (-1)^{k-1}p_{k-1}s_1 + (-1)^k kp_k = 0$$
$$(k = 1, 2, \cdots, n).$$

12. 函数环 令 S 是一个任意非空集合，并令 $\mathfrak{A}$ 是一个任意环. 今論究定义在变区 S 上而变程含于 $\mathfrak{A}$ 里的函数的全体$(\mathfrak{A}, S)$. 則 $(\mathfrak{A}, S)$ 的元素 f 是 S 到 $\mathfrak{A}$ 内的映照 $s \to f(s)$. (必須指出，这里 f 对于 s 的效果規定記作 $f(s)$，而不記作 sf). $f = g$ 的意义是指：对于所有 $s \in S$, $f(s) = g(s)$. 今按常例定义 $(\mathfrak{A}, S)$里加法及乘法为

$$(26)\qquad (f+g)(s) = f(s) + g(s),\quad (fg)(s) = f(s)g(s).$$

容易驗証：$(\mathfrak{A}, S)$ 与这些合成組織成一个环. 这因为，加法及乘法的結合性、加法的交換性、及分配律可由 $\mathfrak{A}$ 里对应的各定律导

出。例如，

$$((f+g)h)(s)=(f(s)+g(s))h(s)$$
$$=f(s)h(s)+g(s)h(s)=(fh+gh)(s).$$

故 $(f+g)h=fh+gh$. 对于所有 s 使 $0(s)=0$ 的函数 0，在加法下有恆等元素的作用，而 $-f$ 是对于所有 s 使 $(-f)(s)=-f(s)$ 的函数.

如果 a 是 $\mathfrak{A}$ 的任一个元素，而对于所有 s 使 $a(s)=a$，則 a 叫做**常值函数**. 这种函数构成 $(\mathfrak{A}, S)$ 的一个子环，与 $\mathfrak{A}$ 是同构的. 这个子环也記作 $\mathfrak{A}$. 如果 $\mathfrak{A}$ 有恆等元素，則与它相应的常值函数在整个环 $(\mathfrak{A}, S)$ 里有恆等元素的作用.

为簡单計，今将假定 $\mathfrak{A}$ 是带恆等元素的交换环. 我們来考究函数环 $\bar{\mathfrak{A}}=(\mathfrak{A}, \mathfrak{A})$. 于常值函数外，添一个特別重要的函数：恆等函数 $s\rightarrow s$. 我們照习慣記法用 s 表这个函数兼表 $\mathfrak{A}$ 里变元 s. 因为 $\mathfrak{A}$ 是可交换的，这函数与常值函数可以交換. 由常值函数及恆等函数生成的环 $\mathfrak{A}[s]$ 的元素叫做**单变元多項函数**. 如果

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

是 $\mathfrak{A}[x]$ 的一个元素，这里 x 是超越的，則 $f(s)$ 是把 s 映到 $\mathfrak{A}$ 里元素 $a_0+a_1s+\cdots+a_ns^n$ 的函数，并且 $\mathfrak{A}[s]$ 是这些函数的全体.

函数 s 毋須是 $\mathfrak{A}$ 上超越元素. 如果 $\mathfrak{A}$ 是拥有元素 $a_1, a_2, \cdots, a_q$ 的一个有限环，則多項式

(27) $$h(x)=(x-a_1)(x-a_2)\cdots(x-a_q)\neq 0,$$

但函数

(28) $$h(s)=(s-a_1)(s-a_2)\cdots(s-a_q)=0,$$

这因为对于所有 $s\in\mathfrak{A}$，显然元素 $h(s)=0$. 我們知道，如果 $\mathfrak{A}$ 是一个有限域，則 $h(x)=x^q-x$（习題 42 第 2 題).

另一方面，我們来驗証：如果 $\mathfrak{A}=\mathfrak{F}$ 是一个无限域，則恆等函数是超越的. 这是定理 7（§ 9）的一个直接推論. 这因为，如果 $f(x)$ 是 $\mathfrak{F}[x]$ 里一个非零多項式，則 $\mathfrak{F}$ 里只有有限个元素能使 $f(s)=0$. 故存在元素 $c\in\mathfrak{F}$，使 $f(c)\neq 0$. 这意味着函数 $f(s)\neq 0$

及 s 是超越的.

多变元多項函数的定义是上面定义的直接推广. 今从 r 維組 $(s_1, s_2, \cdots, s_r)$ 的集合 $S = \mathfrak{A}^{(r)}$ 出发, 这里 $s_i \in \mathfrak{A}$, 并考究函数环 $\bar{\mathfrak{A}}^{(r)} = (\mathfrak{A}, \mathfrak{A}^{(r)})$. 我們在这个环里取由

(29) $$(s_1, s_2, \cdots, s_r) \to s_i$$

定义的特殊函数 s_i, 然后定义 r **变元多項函数**为由常数函数及 r 个函数 s_i 生成的环 $\mathfrak{A}[s_1, s_2, \cdots, s_r]$ 的元素. 显然, s_i 可相互交换,且与常数函数也可交换.

如果 $f(x_1, x_2, \cdots, x_r) \in \mathfrak{A}[x_1, x_2, \cdots, x_r]$, 这里 x_i 是代数无关元素, 則函数 $f(s_1, s_2, \cdots, s_r)$ 的意义是显然的. 这函数是一个多項函数,并且每个多項函数都可依这个方法得出.

如果 $\mathfrak{A}$ 是 q 个元素 a_j 的一个有限环,则

$$h(s_i) = (s_i - a_1)(s_i - a_2)\cdots(s_i - a_q) = 0.$$

故函数 $s_1, s_2, \cdots, s_r$ 关于常值函数的子环是代数相关的. 与这个結果对照,我們将証明: 如果 $\mathfrak{F}$ 是一个无限域,則函数 s_i 是代数无关. 这个結果与下面的定理等价:

定理 10. 如果 $\mathfrak{F}$ 是一个无限域, 并且 $f(x_1, x_2, \cdots, x_r)$ 是多項整区 $\mathfrak{F}[x_1, x_2, \cdots, x_r]$ 里一个非零多項式, x_i 是代數无关元素, 則 $\mathfrak{F}$ 里有元素 $c_1, c_2, \cdots, c_r$ 存在,使 $f(c_1, c_2, \cdots, c_r) \neq 0$.

証 $r=1$ 情形上面已經証明了. 故可假定这定理对于 $r-1$ 个 x 成立. 把 $f(x_1, x_2, \cdots, x_r)$ 写成

$$f(x_1, x_2, \cdots, x_r) = B_0 + B_1x_r + B_2x_r^2 + \cdots + B_nx_r^n,$$

这里 $B_i \in \mathfrak{F}[x_1, x_2, \cdots, x_{r-1}]$. 我們还可設 $B_n \equiv B_n(x_1, x_2, \cdots, x_{r-1}) \neq 0$. 于是,由归納法假設知: $\mathfrak{F}$ 里有元素 c_i 存在,使 $B_n(c_1, c_2, \cdots, c_{r-1}) \neq 0$. 故

$$\begin{aligned} f(c_1, c_2, \cdots, c_{r-1}, x_r) = {} & B_0(c_1, c_2, \cdots, c_{r-1}) \\ & + B_1(c_1, c_2, \cdots, c_{r-1})x_r + \cdots \\ & + B_n(c_1, c_2, \cdots, c_{r-1})x_r^n \neq 0. \end{aligned}$$

所以我們可选取一个値 $x_r = c_r$, 使 $f(c_1, c_2, \cdots, c_r) \neq 0$.

习 題 45

1. 求証定理 10 的拓广定理：如果$f(x_1, x_2, \cdots, x_r)$ 是一个多項式，其系数屬于一个无限域 $\mathfrak{F}$；如果能使另一个非零多項式$g(x_1, x_2, \cdots, x_r)$的値 $g(c_1, c_2, \cdots, c_r) \neq 0$ 的所有 $(c_1, c_2, \cdots, c_r)$ 都使 $f(c_1, c_2, \cdots, c_r) = 0$，則 $f(x_1, x_2, \cdots, x_r) = 0$.

2. 令 $\mathfrak{F}$ 是含有 q 个元素的一个有限域，求証：如果 $f(x_1, x_2, \cdots, x_r)$ 是一个非零多項式，对于每个 x_i 的次数都 $< q$，則 $\mathfrak{F}$ 里存在 c_i，使 $f(c_1, c_2, \cdots, c_r) \neq 0$.

下面各題里的 $\mathfrak{F}$ 都与第2題的 $\mathfrak{F}$ 相同.

3. 求証：每个 r 变元 ($\mathfrak{F}^{(r)}$ 的元素)函数是一个多項函数.

(提示：枚列函数的集合及多項函数的集合.)

4. 驗証：$\mathfrak{F}[x_1, x_2, \cdots, x_r]$ 里任一个多項式可写成形状

$$\sum_{i=1}^{r} g_i(x_1, x_2, \cdots, x_r)(x_i^q - x_i) + g_0(x_1, x_2, \cdots, x_r),$$

这里 g_0 对于每个 x_i 的次数 $< q$.

5. 求証：如果 $m(x_1, x_2, \cdots, x_r)$ 是一个多項式，使函数 $m(s_1, s_2, \cdots, s_r) = 0$，則 $m(x_1, x_2, \cdots, x_r)$ 可写成形状 $\Sigma g_i(x_1, x_2, \cdots, x_r)(x_i^q - x_i)$.

6. 令 $f(x_1, x_2, \cdots, x_r)$ 是一个多項式，使 $f(0, 0, \cdots, 0) = 0$，并且对于所有

$$(c_1, c_2, \cdots, c_r) \neq (0, 0, \cdots, 0),$$

都有 $f(c_1, c_2, \cdots, c_r) \neq 0$. 求証：如果

$$F(x_1, x_2, \cdots, x_r) = 1 - f(x_1, x_2, \cdots, x_r)^{q-1},$$

則当 $(c_1, c_2, \cdots, c_r) = (0, 0, \cdots, 0)$ 时，$F(c_1, c_2, \cdots, c_r) = 1$；在其他情形时 $F(c_1, c_2, \cdots, c_r) = 0$.

7. 驗証：第 6 題的 F 与

$$F_0 = (1 - x_1^{q-1})(1 - x_2^{q-1})\cdots(1 - x_r^{q-1})$$

决定同一函数. 于是証明：$\deg F \geqslant r(q - 1)$（这里，$\deg F = F$ 的总次数).

8. 求証阿廷-捷发莱 (Artin-Chevalley)定理：令 $f(x_1, x_2, \cdots, x_r)$ 是 n ($< r$) 次多項式，并設 $f(0, 0, \cdots, 0) = 0$. 則有一个 $(c_1, c_2, \cdots, c_r) \neq (0, 0, \cdots, 0)$ 存在使 $f(c_1, c_2, \cdots, c_r) = 0$.

第　四　章

因子分解的初等理論

本章論究一个給定交換整区的元素分解为不可約元素之积的問題．在若干重要整区里，这样因子分解对于所有非单位元素是存在的，且在某种意义下，因子分解的唯一性成立．在这些事例里我們可决定一个給定元素的所有因子，从而可得关于 $ax=b$ 形方程的可解性的簡单条件．因为这里要討論的因子分解的理論是与一个交換整区里非零元素的半羣相牵連的一个純粹乘法理論．故我們从半羣的因子分解理論說起，更易明了．

1．因子，相伴元素，不可約元素　令 $\mathfrak{S}$ 是一个任意交換半羣，拥有一个恆等元素 1，幷适合相消律．如果 $\mathfrak{U}$ 表 $\mathfrak{S}$ 的单位元素的集合，則知 $\mathfrak{U}$ 是 $\mathfrak{S}$ 的一个子羣．

如果 a 及 b 是 $\mathfrak{S}$ 的元素，幷且 $\mathfrak{S}$ 里存在一个元素 c 使 $a=bc$，則 b 叫做 a 的一个因子，或除式．如果 b 是 a 的一个因子，我們記作 $b|a$．这种关系易知是传递的，幷且是反身的．元素 u 是一个单位元素，必須而且只須 $u|1$．因为单位元素是 $\mathfrak{S}$ 的每个元素的因子，故它們是当然因子．如果 $a|b$，幷且 $b|a$，这种元素叫做相伴元素．对于这种关系的条件是：$b=au, a=bv$，故 $b=au=bvu$．由相消律得 $vu=1$．故 a 与 b 的差别只是单位元素的因子．逆定理也易知成立；幷且相伴性是一个等价关系也是显然的．如果 a 与 b 是相伴元素，則記作 $a\sim b$．

如果 $b|a$，幷且 b 不是一个单位元素，也不是 a 的相伴元素，則說 b 是 a 的眞因子；此时，$a=bc$，而 c 既不是单位元素，也不是 a 的相伴元素．故 c 也是 a 的一个眞因子．如果 u 是单位元素，而 $u=vw$，則易知 v 及 w 都是单位元素．故 $\mathfrak{S}$ 的单位元素

无眞因子.

如果 a 不是单位元素,并且在 $\mathfrak{S}$ 里无眞因子,则 a 叫做**不可約元素**.

2. 高斯半羣 如果交换半羣 $\mathfrak{S}$ 的一个元素 a 有一个因子分解 $a = p_1 p_2 \cdots p_s$, 这里 p_i 是不可約元素, 则 a 还有因子分解 $a = p_1' p_2' \cdots p_s'$, 这里 $p_i' = u_i p_i$, 而 u_i 是使 $u_1 u_2 \cdots u_s = 1$ 的单位元素. 显然 p_i' 是不可約的. 所以, 如果 $\mathfrak{S}$ 有 $\neq 1$ 的单位元素, 并且 $s > 1$, 则常可如上面指出的方式改变一个因子分解, 以得出給定元素的其他因子分解. 新的因子分解被認为与原来的因子分解实質上相同; 并且 a 分解为不可約元素的一个因子分解 $a = p_1 p_2 \cdots p_s$ 后, 如果还有任意其他分解为不可約元素 p_i' 的因子分解 $a = p_1' p_2' \cdots p_t'$ 就必須 $t = s$, 而且 p_i' 經过适宜改編后有 $p_i' \sim p_i$ 时, 则我們說 $a = p_1 p_2 \cdots p_s$ 是**实質上唯一的**因子分解. 今使用这个概念来述下面的定义.

定义 1. 如果(1)半羣 $\mathfrak{S}$ 是可交换的, 拥有一个恆等元素, 并且适合相消律; (2)它的每个非单位元素可分解为不可約元素的因子分解, 且实質上唯一的, 则 $\mathfrak{S}$ 叫做**高斯(Gauss)半羣**. 如果一个整区里非零元素的半羣是高斯半羣, 则这个整区叫做**高斯整区**.

本章的主要目的是驗証: 若干重要类型的整区都是高斯整区. 至于这性質不是每个整区所通有, 可由下面的例子看出.

例. 令 $\mathfrak{A} = I[\sqrt{-5}]$, 这是形状如 $a + b\sqrt{-5}$ 的复数的集合, 这里 a 及 b 是整数. 我們易知, $\mathfrak{A}$ 是复数域的一个子环, 故 $\mathfrak{A}$ 是一个交换整区. $\mathfrak{A}$ 还有恆等元素 $1 = 1 + 0\sqrt{-5}$.

$\mathfrak{A}$ 的算术的考究可由介紹这整区的元素的距而大为省事: 如果 $r = a + b\sqrt{-5}$, 我們定义 r 的距是 $N(r) = r\bar{r} = a^2 + 5b^2$. 它是乘法函数, 即: $N(rs) = N(r)N(s)$. 对于 $\mathfrak{A}$ 里非零元素, 距的値都是正整数.

我們先用距来决定 $\mathfrak{A}$ 的单位元素. 如果 $rs = 1$, 则 $N(r)N(s) = N(1) = 1$, 故 $N(r) = a^2 + 5b^2 = 1$. 于是, $a = \pm 1$, 而 $b = 0$. 故 $r = \pm 1$.

由此可見, $\mathfrak{A}$ 里一个元素的唯一相伴元素是它自身及它的負元素.

今考究两种因子分解

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

因子 3 及 $2 \pm \sqrt{-5}$ 都是不可約的. 这因为, 假設 $3 = rs$, 则 $9 = N(3) = N(r)N(s)$. 于是, $N(r) = 1, 3$, 或 9. 但, 如果 $N(r) = 3$, 则 $a^2 + 5b^2 = 3$, 此时要 a 及 b 为

整数是不可能的。故 $N(r)=1$，或者 $N(r)=9$ 而 $N(s)=1$．由前者得 $r=1$，由后者得 $s=1$．同理可知 $2\pm\sqrt{-5}$ 也是不可約的．故此时分解为不可約元素有实質上不同的两种分解，故 $\mathfrak{A}$ 不是高斯整区．

在任一个高斯半羣 $\mathfrak{S}$ 里，假定一个給定的非单位元素 a 分解为不可約元素的因子分解是已知时，則我們除单位因子不計外，可决定 a 的所有因子．这因为，如果 $a=p_1p_2\cdots p_s$，这里 p_i 是不可約元素，并且如果 $a=bc$，这里 $b=p_1'p_2'\cdots p_t'$，$c=p_1''p_2''\cdots p_u''$，而 p_j' 及 p_k'' 都是不可約元素，則

$$a=p_1p_2\cdots p_s=p_1'p_2'\cdots p_t'p_1''p_2''\cdots p_u'',$$

由唯一性知：$p_j'\sim p_{i_j}$，这里 $j\neq k$ 时 $i_j\neq i_k$．于是，$b\sim p_{i_1}p_{i_2}\cdots p_{i_t}$．故 a 的任一个因子是由这样得来 2^s 个积中的一个的相伴元素．如果 a 的不可約因子的个数 s 叫做 a 的长，則还知道：a 的任一个真因子的长必比 a 的长小．故任一个高斯半羣显然适合下面的条件：

A．（因子鏈条件）．$\mathfrak{S}$ 不能含有这样的无限序列 $a_1,a_2,\cdots$，这里每个 a_{i+1} 是 a_i 的一个真因子．

今将驗証由这个条件及另一个条件就可确定拥有恆等元素及相消律的交換半羣是高斯半羣．这另一个条件含有素元素的概念．如果 $\mathfrak{S}$ 的一个元素 p 能除尽任一个积 ab，則必能除尽 a 与 b 中的一个；具有这样性质的元素 p 叫做**素元素**．于是，另一个条件可述如次：

B．$\mathfrak{S}$ 的每个不可約元素是素元素．

条件 A 保証 $\mathfrak{S}$ 里任一个非单位元素分解为不可約元素的一个因子分解的存在．令 a 是一个非单位元素，今先驗証 a 有一个不可約因子．如果 a 自身是不可約的，則无須証明了；否則，令 $a=a_1b_1$，这里 a_1 是一个真因子．継續这样下去，就得一个序列，其中每个 a_i 是 a_{i-1} 的一个真因子．由 A 知，經过有限次进行后，就应該停止下来．如果 a_n 是末項，則 a_n 是不可約的，并且 $a_n|a$．

今令 $a_n=p_1$，写 $a=p_1a'$．如果 a' 是一个单位元素，則 a 是不可約的．否則，$a'=p_2a''$，这里 p_2 是不可約的．継續这样

下去，序列 $a, a', a'', \cdots$ 里每个都是前一个的眞因子，并且每个 $a^{(i-1)} = p_i a^{(i)}$，而 p_i 是不可約的．这方法于达到一个不可約元素 $a^{(s-1)} = p_s$ 时終止．于是，

$$a = p_1 a' = p_1 p_2 a'' = \cdots = p_1 p_2 \cdots p_s,$$

这里 p_i 是不可約的．

其次，我們要驗証：条件 B 保証分解为不可約元素的因子分解的唯一性．这因为，令

(1) $$a = p_1 p_2 \cdots p_s = p_1' p_2' \cdots p_t'$$

是同一个元素分解为不可約因子的两种因子分解，并設任一个元素分解为 $s-1$ 个不可約元素的因子分解时，实質上这种分解是唯一的．于是，因为(1)里元素 p_1 是不可約的，故由 B 知它是素元素．簡单的归納法論証指出：如果 p_1 可除尽二个以上的因子之积，則必能除尽其中一个因子．由此可推得 p_1 可除尽 p_i' 中的一个．我們如果在必要时把 p' 改編，就不妨假定 p_1' 可被 p_1 除尽．因为 p_1 与 p_1' 都是不可約的，故 $p_1' \sim p_1$．于是，$p_1' = p_1 u_1$，这里 u_1 是一个单位元素．以此代入(1)的第二种因子分解里，并把 p_1 相消，得

$$p_2 p_3 \cdots p_s = u_1 p_2' p_3' \cdots p_t'.$$

令

$$u_1 p_2' = p_2'',\ p_3' = p_3'', \cdots,\ p_t' = p_t'',$$

則

$$p_2 p_3 \cdots p_s = p_2'' p_3'' \cdots p_t'',$$

这里 p_i'' 是不可約的．由归納法假設得 $s-1 = t-1$，并且在 p_i'' 适当改編后得 $p_i'' \sim p_i$．故 $s = t$，并且 $p_i' \sim p_i'' \sim p_i$ $(i = 2, 3, \cdots, s)$．

习　　題 46

1．驗証：$I[\sqrt{-5}]$ 适合 A．

2．令 $\mathfrak{A}$ 是 $a_1 x^{\alpha_1} + a_2 x^{\alpha_2} + \cdots + a_n x^{\alpha_n}$ 的集合，这里 a_i 是域 $\mathfrak{F}$ 里任意元素，而 α_i 是非負的有理数．依普通方式定义加法，并以 $x^\alpha x^\beta = x^{\alpha+\beta}$ 定义乘法．驗証：$\mathfrak{A}$ 是带恆等元素的一个交換整区；并驗証：$\mathfrak{A}$ 的元素 x 不是一个单位元素，但这元素

不能分解为不可約元素.

3. 驗証:条件B在任一个高斯半羣里成立.

3. 最大公因子 令 a 是高斯半羣 $\mathfrak{S}$ 的一个元素. 設在 a 的因子分解里把相伴的不可約因子合併起来,得一个因子分解

(2) $$a = up_1^{e_1}p_2^{e_2}\cdots p_r^{e_r},$$

此时,不可約元素 $p_1,\cdots,p_r$ 里沒有两个是相伴的, e_i 是正整数, u 是一个单位元素. 显然, a 的因子的形状是 $u'p_1^{e_1'}p_2^{e_2'}\cdots p_r^{e_r'}$, 这里 u' 是一个单位元素,而 e_i' 是适合 $0 \leqslant e_i' \leqslant e_i$ 的整数.

我們还易知:如果 a 及 b 是任意两个非单位元素,則可用同样的非相伴元素表出,亦即可写成

$$a = up_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}, \quad b = vp_1^{f_1}p_2^{f_2}\cdots p_t^{f_t},$$

这里 u 及 v 是单位元素,而 e_i 及 f_i 都是 $\geqslant 0$。今考究元素

$$d = p_1^{g_1}p_2^{g_2}\cdots p_t^{g_t}, \quad g_i = \min(e_i, f_i),$$

显然 $d|a, d|b$。再則,如果 $c|a$, $c|b$, 則 $c = wp_1^{k_1}p_2^{k_2}\cdots p_t^{k_t}$,这里 w 是一个单位元素,而 $k_i \leqslant e_i, f_i$; 故 $k_i \leqslant g_i$, 并且 $c|d$. 这意味着,元素 d 按下列的定义是 a 与 b 的最大公因子.

定义 2. 如果 $\mathfrak{S}$ 的元素 d 对于元素 a,b 适合 $d|a$ 及 $d|b$, 并且任一个元素 c 适合 $c|a$ 及 $c|b$, 就一定是 d 的因子时, d 叫做 a 与 b 的**最大公因子**(簡写作 g. c. d.).

如果 d 是 a 与 b 的最大公因子, 則 ud 也是 a 与 b 的最大公因子,这里 u 是一个单位元素. 反过来, 如果 d' 是 a 与 b 的任一个最大公因子, 則 $d|d'$, 并且 $d'|d$, 故 $d \sim d'$. 于是, 最大公因子除一个单位因子的差别外,是完全决定的. 为方便計, a 与 b 的任一个最大公因子記作(a,b).

今将驗証: 任意半羣 $\mathfrak{S}$ 里, 从每两个元素的最大公因子的存在可推得 $\mathfrak{S}$ 适合条件 B. 因此,設 $\mathfrak{S}$ 是拥有恆等元素及相消律的任一个交換羣,使

C. $\mathfrak{S}$ 里每两个元素 a, b 在 $\mathfrak{S}$ 里有一个最大公因子.

我們要驗証: $\mathfrak{S}$ 里每个不可約元素是素元素. 欲达到这目的,需要几个簡单引理.

引理 1. 如果条件C在 $\mathfrak{S}$ 里成立，则 $\mathfrak{S}$ 里任意有限个元素必有一个最大公因子.

令 $a,b,c \in \mathfrak{S}$，并令 $r=(a,(b,c))$. 则 $r|a$，并且 $r|(b,c)$，从而 $r|b$，$r|c$. 又若 $s|a,b,c$，则 $s|a$，并且 $s|(b,c)$，故 $s|(a,(b,c))$. 这指出 $r=(a,(b,c))$ 是 a,b 及 c 的一个最大公因子. 类似論証对于三个以上的元素也成立. 再则 $((a,b),c)$ 显然也是 a,b 及 c 的一个最大公因子. 这証明了

引理 2. $(a,(b,c))\sim((a,b),c)$.

其次，証明

引理 3. $c(a,b)\sim(ca,cb)$.

証 令 $d=(a,b)$ 及 $e=(ca,cb)$，则 $cd|ca$，$cd|cb$；故 $cd|e$. 反过来，因 $ca=ex$，及 $cb=ey$. 如果 $e=cdu$，则

$$ca=cdux,\quad cb=cduy.$$

故 $a=dux$，$b=duy$. 因此，$du|a$，$du|b$. 故 $du|d$. 而 u 是一个单位元素. 这証明了 $c(a,b)\sim(ca,cb)$.

引理 4. 如果 $(a,b)\sim1$，及 $(a,c)\sim1$，则 $(a,bc)\sim1$.

証 如果 $(a,b)\sim1$，则 $(ac,bc)\sim c$. 故 $1\sim(a,c)\sim(a,(ac,bc))\sim((a,ac),bc)\sim(a,bc)$.

今設 p 是不可約的，并設 a 与 b 是 $\mathfrak{S}$ 的元素使 $p|ab$. 因为 p 是不可約的，而 (p,a) 是 a 的一个因子，故 $(p,a)\sim p$，或者 $(p,a)\sim1$. 同理，$(p,b)\sim p$，或者 $(p,b)\sim1$. 但从 $(p,a)\sim1$ 及 $(p,b)\sim1$ 可由引理 4 导出 $(p,ab)\sim1$，这与 $(p,ab)\sim p$ 矛盾. 故 $(p,a)\sim p$，或者 $(p,b)\sim p$. 于是，$p|a$，或者 $p|b$. 这証明了条件 B. 由前节結果，得下面的定理.

定理 1. 如果 $\mathfrak{S}$ 是一个拥有恒等元素及相消律的交换半羣，并且 $\mathfrak{S}$ 适合A及C，则 $\mathfrak{S}$ 是高斯半羣.

由引論知，正整数及整数整区的半羣具有最大公因子的性質 C. 又由絕对值的考究，易知A在这些代数系里也成立. 故它們是高斯整区.

习　题　47

1. 如果元素 m 对于元素 a,b 具有 $a|m$, $b|m$，并且适合 $a|n$, $b|n$ 的任一个元素 n 一定有 $m|n$ 时，则 m 叫做 a 及 b 的最小公倍(簡写作 l.c.m.)。求証：高斯整环里任意两个元素有一个 l.c.m.。

2. 如果 $\mathfrak{S}$ 是高斯整区。令 $[a,b]$ 表 a 及 b 的一个 l.c.m.，求証：$(a,b)[a,b]\sim ab$；并証：$[a,(b,c)]=([a,b],[a,c])$。

3. 如果 p 是一个正素数，求証：二項式系数

$$\binom{p}{i}=\frac{p!}{i!(p-i)!}(1\leqslant i\leqslant p-1)$$

可被 p 整除。由此証明：特征数 p 的任一个交換环里，对于所有 a 及 b，

$$(a+b)^p=a^p+b^p$$

成立。

4. 正整数的默比烏斯 (Möbius) 函数 $\mu(n)$ 定义为：$(a)\mu(1)=1$，(b) 如果 n 有平方因子，則 $\mu(n)=0$，(c) 如果 n 不含有平方因子，而 s 是 n 的长，則 $\mu(n)=(-1)^s$。求证：$\mu(n)$ 是乘法函数，亦即：如果 $(n_1,n_2)=1$，則 $\mu(n_1n_2)=\mu(n_1)\mu(n_2)$；并証

$$\sum_{d\mid n}\mu(d)=\begin{cases}1\ (n=1\text{ 时}),\\ 0\ (n>1\text{ 时}).\end{cases}$$

5. 証明：默比烏斯反演公式：如果 $f(n)$ 是正整数的一个函数，其值属于一个环里，并且

$$g(n)=\sum_{d\mid n}f(d),$$

則

$$f(n)=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)g(d).$$

6. 如果 $\phi(n)$ 是欧拉 ϕ 函数，求証

$$\phi(n)=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)d.$$

(参看习題 13 第 3 題)。

4. 主理想整区　令 $\mathfrak{A}$ 是带恆等元素的交換整区。我們曾把主理想 (b) 定义为 $\mathfrak{A}$ 里含有元素 b 的最小理想。因为 $\mathfrak{A}$ 有一个恆等元素，故 (b) 与元素 b 的倍数 bx 的全体重合。但 $b|a$ 意味着 $a=bc\in(b)$，而这結果与要求 $(a)\subseteq(b)$ 是等价的。我們还得指出：如果 $(a)=(b)$，則 $b|a$，并且 $a|b$，故 $a\sim b$。反过来也是眞的。故知：b 是 a 的一个眞因子必須而且只須 $(a)\subset(b)$。故关于整区 $\mathfrak{A}$ 的因子鏈条件 A 可說成下面关于理想的鏈条件：

A′. $\mathfrak{A}$ 不含有无限眞上升理想链 $(a_1)\subset(a_2)\subset(a_3)\subset\cdots$。

如果一个带恆等元素的交換整区 $\mathfrak{A}$ 所含的理想都是主理想，这种整区叫做主理想整区．今将考究这种整区．本节要証明：每个主理想整区是高斯整区．

首先証明 A′．令 $(a_1)\subseteq(a_2)\subseteq(a_3)\subseteq\cdots$ 是 $\mathfrak{A}$ 里一个无限上升理想鏈．令 $\mathfrak{B}=\cup(a_i)$ 是集合(a_i)的併集，則 $\mathfrak{B}$ 是 $\mathfrak{A}$ 里一个理想．这因为，令 $b_1,b_2\in\mathfrak{B}$，則 $b_1\in(a_k),b_2\in(a_l)$．我們可設 $k\leqslant l$．于是，$b_1,b_2\in(a_l)$．故 $b_1-b_2\in(a_l)$，并且对于任一个 $x,b_1x\in(a_l)$．故 b_1-b_2 及 b_1x 都属于 $\mathfrak{B}$．这就可見：$\mathfrak{B}$ 是一个理想．但由假設，$\mathfrak{B}=(d)$，这里 $d\in\mathfrak{B}$．因为 $d\in\mathfrak{B}$，故有一个整数 n 存在，使 $d\in(a_n)$．于是 $\mathfrak{B}=(d)=(a_n)$．所以，如果 $m\geqslant n$，則

$$(a_m)\supseteq(a_n)=\mathfrak{B}\supseteq(a_m).$$

因此 $(a_m)=(a_n)$．这証明了 $\mathfrak{A}$ 不能含有眞上升理想的无限序列．

次令 a 及 b 是 $\mathfrak{A}$ 的任意两个元素，并令 (a,b) 表示由 a 及 b 生成的理想 $(a)+(b)$．这个理想是元素 $ax+by$ 的全体，这里 x 及 $y\in\mathfrak{A}$．但$(a,b)=(d)$．因为 $(d)\supseteq(a)$，并且 $(d)\supseteq(b)$，故 $d|a$，并且 $d|b$．另一方面，如果 $e|a,e|b$，則$(e)\supseteq(a),(e)\supseteq(b)$．于是，$(e)\supseteq(d)$；从而，$e|d$．这証明 d 是 a 及 b 的最大公因子．故 C 成立．于是，得下面的定理．

定理 2. 每个主理想整区是高斯整区．

我們已知，如果 $\mathfrak{F}$ 是一个域，x 是超越元素，則 $\mathfrak{F}[x]$ 是一个主理想整区（第三章，§6）．故 $\mathfrak{F}[x]$ 是高斯整区．

习 題 48

1．求証：交換整区 $\mathfrak{A}$ 的一个元素 p 是一个素元素，必須而且只須 $\mathfrak{A}/(p)$ 是一个整区．

2．如果在一个主理想整区里，p 是一个素元素，求証：$\mathfrak{A}/(p)$ 是一个域．

3．令 $\mathfrak{A}$ 是一个主理想整区，$\mathfrak{B}$ 是包含 $\mathfrak{A}$ 的任一个交換整区．如果 $a,b\in\mathfrak{A}$ 有最大公因子 $d\in\mathfrak{A}$，驗証：在 $\mathfrak{B}$ 里 d 是 a 及 b 的一个最大公因子．

4．令 $\mathfrak{F}$ 是含有 q 个元素的一个有限域，$N(r,q)$ 表 $\mathfrak{F}[x]$ 里 r 次不可約多項式的个数．求决定 $N(2,q)$ 及 $N(3,q)$．

5．如果 $\mathfrak{A}$ 是带恆等元素的一个交換整区，但不是一个域．求証：$\mathfrak{A}[x]$ 不是一个主理想整区．

5. 欧几里得整区 在整数环 I 里，函数 $\delta(a)=|a|$ 适合次列各条件：

1. $\delta(a)$ 是一个非負整数，$\delta(a)=0$ 必須而且只須 $a=0$。

2. $\delta(ab)=\delta(a)\delta(b)$.

3. 如果 $b\neq 0$，而 a 是任意整数，則有元素 q 及 r 存在，使 $a=bq+r$，这里 $\delta(r)<\delta(b)$.

設 $\mathfrak{F}$ 是一个域，而 x 是超越元素，則在任一个多項式整区 $\mathfrak{F}[x]$ 里可定义类似的函数。此时，取 $\delta(a(x))=2^{\deg a(x)}$，則易知条件 1 及 2 成立，而 3 等价于前面討論过的除法算法。环 I 及 $\mathfrak{F}[x]$ 都是下面定义的欧几里得整区的例子。

定义 3. 如果在带恆等元素的一个交換整区 $\mathfrak{A}$ 里能够定义一个函数 $\delta(a)$，适合上面的 1, 2, 3 三个条件，則 $\mathfrak{A}$ 叫做**欧几里得(Euclid)整区**.

現在再給出欧几里得整区的另一个例子：$I[\sqrt{-1}]$，卽形状如 $m+n\sqrt{-1}$ 的复数的全部，这里 m 及 n 是整数。这类型的数叫做**高斯整数**. 設 $a=m+n\sqrt{-1}$，令 $\delta(a)=|a|^2=m^2+n^2$，則 $\delta(a)$ 显然适合 1 及 2．今令 a 及 $b(\neq 0)$ 属于 $I[\sqrt{-1}]$，則复数 $ab^{-1}=\mu+\nu\sqrt{-1}$，这里 μ 及 ν 是有理数。我們可覓得整数 u 及 v 使 $|u-\mu|\leqslant\frac{1}{2}$，$|v-\nu|\leqslant\frac{1}{2}$. 令 $\varepsilon=\mu-u$, $\eta=\nu-v$，則 $|\varepsilon|\leqslant\frac{1}{2}$，$|\eta|\leqslant\frac{1}{2}$. 于是，

$$\begin{aligned}a&=b[(u+\varepsilon)+(v+\eta)\sqrt{-1}]\\&=bq+r,\end{aligned}$$

这里 $q=u+v\sqrt{-1}\in I[\sqrt{-1}]$，而 $r=b(\varepsilon+\eta\sqrt{-1})$. 因为 $r=a-bq$，故 $r\in I[\sqrt{-1}]$．又因为

$$\delta(r)=|r|^2=|b|^2(\varepsilon^2+\eta^2)\leqslant|b|^2\left(\frac{1}{4}+\frac{1}{4}\right)=\frac{1}{2}\delta(b),$$

故 $\delta(r)<\delta(b)$.

关于欧几里得整区的主要結果是下面的定理。

定理 3. 每个歐几里得整区是一个主理想整区.

証 令 $\mathfrak{B}$ 是欧几里得整区 $\mathfrak{A}$ 里任一个理想. 如果 $\mathfrak{B}=0$, 則 $\mathfrak{B}=(0)$. 今令 $\mathfrak{B}\neq 0$, 則 $\mathfrak{B}$ 必含有元素, 它的 $\delta>0$. 又因为 δ 是非負的整数, 故存在一个 $b\in\mathfrak{B}$, 使对于 $\mathfrak{B}$ 里每个 $c\neq 0$ 有 $0<\delta(b)\leqslant\delta(c)$. 如果 c 是 $\mathfrak{B}$ 的任意一个元素, 則可写做 $c=bq+r$, 这里 $\delta(r)<\delta(b)$. 但因为 $\mathfrak{B}$ 是一个理想, 故 $r=c-bq\in\mathfrak{B}$. 由于 $\delta(b)$ 是$\mathfrak{B}$的非零元素里最小的正 δ, 今又有 $\delta(r)<\delta(b)$, 故只能 $r=0$. 于是, $c=bq\in(b)$. 故 $\mathfrak{B}=(b)$, 这就完成了証明.

因为每个主理想整区是高斯整区, 故得

系. 每个歐几里得整区是高斯整区.[1)]

习 題 49

1. 求証: 形状如 $m+n\sqrt{2}$ 的实数集合 $I[\sqrt{2}]$ 是欧几里得整区, 这里 m,n 是整数.

2. 令 $\mathfrak{A}$ 是复数 $m+n\sqrt{-3}$ 的全体, 这里 m 及 n 或者都是整数, 或者都是奇数的 $\frac{1}{2}$. 驗証: $\mathfrak{A}$ 对于通常的加法及乘法成一个环. 求証: $\mathfrak{A}$ 是欧几里得整区.

3. 求証: 欧几里得整区的一个元素 a 是单位元素必須而且只須 $\delta(a)=1$.

4. 令$\mathfrak{A}$是一个欧几里得整区, 它的函数适合条件 $\delta(a+b)\leqslant\max(\delta(a),\ \delta(b))$. 驗証: $\mathfrak{A}$ 或是一个域. 或是域 $\mathfrak{F}$ 上一个多項式整区 $\mathfrak{F}[x]$.

6. 高斯整区的多項式扩张 本节将証明重要的定理: 如果 $\mathfrak{A}$ 是高斯整区, 而 x 是超越元素, 則 $\mathfrak{A}[x]$ 是高斯整区.

令 $f(x)=a_0+a_1x+\cdots+a_nx^n\neq 0$ 属于 $\mathfrak{A}[x]$, 并令 d 是所有非零系数 a_i 的最大公因子. 令 $a_i=da_i'$; 于是, $f(x)=df_1(x)$, 这里

$$f_1(x)=a_0'+a_1'x+\cdots+a_n'x^n.$$

非零系数 a_i' 的最大公因子显然是 1 (或是单位元素). 具有这个性質的多項式叫做**原多項式**. 今設 $f(x)=ef_2(x)$是 $f(x)$分解为一个常数 e ($\mathfrak{A}$ 的元素) 与一个原多項式之积的任一个因子分解. 則 e 是 $f(x)$的系数的一个公因子, 故 $e\mid d$. 令 $d=ek$, 則 $f_2(x)=$

1) 关于欧几里得整区的其他結果見第六章 §10. ——著者注.

$kf_1(x)$. 因为 $f_2(x)$是原多項式,故 k 是一个单位元素. 于是,任一个非零多项式写成一个常数与一个原多項式之积实質上只有一种方法.

在討論 $\mathfrak{A}[x]$中,引入多项式环 $\mathfrak{F}[x]$是有好处的,这里 $\mathfrak{F}$ 是 $\mathfrak{A}$ 的分式域. 今証下面的引理.

引理 1. 如果 $f_1(x)$ 及 $f_2(x)$是 $\mathfrak{A}[x]$ 里原多項式, 且在 $\mathfrak{F}[x]$ 里是相伴元素,則它們在 $\mathfrak{A}[x]$ 里也是相伴元素.

証 因为 $\mathfrak{F}[x]$ 的单位元素是 $\mathfrak{F}$ 里非零元素, 故 $f_1(x) = \alpha f_2(x), \alpha \neq 0$ 且 $\alpha \in \mathfrak{F}$. 令$\alpha = d_2 d_1^{-1}$, $d_i \in \mathfrak{A}$,則 $d_1 f_1(x) = d_2 f_2(x)$. 这就使 $\mathfrak{A}[x]$里一个多项式可有两种方法写做一个常数与一个原多項式之积了. 故知 d_1 与 d_2 的差别只能是 $\mathfrak{A}$ 里一个单位因子. 故 $f_1(x)$ 与 $f_2(x)$在 $\mathfrak{A}[x]$ 里只有一个单位因子的差别.

要証 $\mathfrak{A}[x]$ 是高斯整区,关鍵在証下面的引理.

引理 2.(高斯引理) 原多項式的積是原多項式.

証 令 $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ 及 $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ 是原多項式. 并設 $f(x)g(x) = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n}$ 不是原多項式. 則有一个不可約元素 $p \in \mathfrak{A}$ 存在,使 $p | c_i (i = 0, 1, \cdots, m+n)$. 因为 $f(x)$是原多項式,故 p 不是所有 a_i 的因子;設 $a_{n'}$ 是最后一个 a_i 不能被 p 除尽. 同样,令 $b_{m'}$ 是最后一个 b_i 不能被 p 除尽. 今考究系数

$$c_{m'+n'} = a_0 b_{m'+n'} + a_1 b_{m'+n'-1} + \cdots + a_{n'-1} b_{m'+1} + a_{n'} b_{m'} + a_{n'+1} b_{m'-1} + \cdots + a_{m'+n'} b_0.$$

因为在項 $a_{n'} b_{m'}$ 前面各項里所有 b_i 都可被 p 除尽,而这項后面各項里所有 a_j 都可被 p 除尽,还有 $c_{m'+n'}$ 也可被 p 除尽,故 $p | a_{n'} b_{m'}$. 但 p 不是 $a_{n'}$ 或 $b_{m'}$ 的因子,这与 p 是不可約的而且也是素元素的事实矛盾(参看习题 46 第 3 題).

高斯引理的一个推論是

引理 3. 如果 $f(x)$ 是 $\mathfrak{A}[x]$ 里一个不可約多項式, 它的次數 >0,則 $f(x)$ 在 $\mathfrak{F}[x]$ 里也是不可約的.

証 因为 $f(x)$是不可約的, 故它是原多項式. 今令 $f(x)$ 是

$\mathfrak{A}[x]$里任一个原多項式，并設在 $\mathfrak{F}[x]$ 里 $f(x)=\phi_1(x)\phi_2(x)$，这里 $\deg\phi_i(x)>0$. 因为，如果 $\phi(x)$是 $\mathfrak{F}[x]$ 里任一个多項式 $\neq 0$，令 $\phi(x)$的系数是 $\alpha_j=a_jb_j^{-1}$，这里 $a_j,b_j\in\mathfrak{A}$. 则可令

$$\alpha_j=(a_jb_0\cdots b_{j-1}b_{j+1}\cdots b_n)(b_0b_1\cdots b_n)^{-1};$$

这就把 α_j 写成有公分母 $b=b_0b_1\cdots b_n$ 的分式. 故 $\phi(x)=b^{-1}g(x)$，这里 $g(x)\in\mathfrak{A}[x]$. 我們还可写 $g(x)=ch(x)$，这里 $c\in\mathfrak{A}$，而 $h(x)$ 是原多項式. 于是，$\phi(x)=b^{-1}ch(x)$. 把这些討論应用于 $\phi_i(x)$，得 $\phi_i(x)=b_i^{-1}c_ih_i(x)$. 于是，

$$f(x)=b_1^{-1}b_2^{-1}c_1c_2h_1(x)h_2(x),$$

而

$$b_1b_2f(x)=c_1c_2h_1(x)h_2(x).$$

因为 $h_i(x)$是原多項式，故 $h_1(x)h_2(x)$ 是原多項式. 于是，$f(x)\sim h_1(x)h_2(x)$，并且我們可設 $f(x)=h_1(x)h_2(x)$. 因为 $\deg h_i(x)=\deg\phi_i(x)>0$，所以这是 $f(x)$ 在 $\mathfrak{A}[x]$ 里的一个眞因子分解. 故知，如果 $f(x)$ 在 $\mathfrak{A}[x]$ 里是不可約时，則它在 $\mathfrak{F}[x]$ 里仍是不可約的.

至此可証主要的結論：

定理 4. 如果 $\mathfrak{A}$ 是高斯整区，而 x 是 $\mathfrak{A}$ 上超越元素，則 $\mathfrak{A}[x]$ 是高斯整区.

証 令 $f(x)\neq 0$，并且不等于一个单位元素，則 $f(x)=df_1(x)$，这里 $f_1(x)$ 是原多項式，而 d 是一个常数. 如果 $f_1(x)$ 不是一个单位元素，并且是可約的，則 $f_1(x)=f_{11}(x)f_{12}(x)$. 显然，$f_{1i}(x)$有正次数. 故 $\deg f_{1i}(x)<\deg f_1(x)$. 这样継續下去，得 $f_1(x)$ 的一个因子分解为

$$f_1(x)=q_1(x)q_2(x)\cdots q_h(x),$$

这里 $q_i(x)$ 是不可約的，并且有正次数. 我們还可把 d 分解为 $d=p_1p_2\cdots p_s$，这里 p_i 是 $\mathfrak{A}$ 里不可約元素，从而也是 $\mathfrak{A}[x]$ 里不可約元素. 这就得出 $f(x)$分解为 $\mathfrak{A}[x]$里不可約元素的因子分解. 今设

$$f(x)=p_1p_2\cdots p_sq_1(x)q_2(x)\cdots q_h(x) \tag{4}$$

$$= p_1'p_2'\cdots p_t'q_1'(x)q_2'(x)\cdots q_k'(x)$$

是 $f(x)$ 分解为不可約因子的两种因子分解，并設我們采取的記法要使 $\deg q_i(x) > 0$，$\deg q_i'(x) > 0$，$p_i, p_i' \in \mathfrak{A}$. 于是，$q_i(x)$ 及 $q_i'(x)$是原多項式．故 $q_1(x)q_2(x)\cdots q_h(x)$ 及 $q_1'(x)q_2'(x)\cdots q_k'(x)$ 是原多項式．由此可見这两个积成相伴元素；并且用单位元素改变其中一个后，我們可設 $\Pi q_i(x) = \Pi q_i'(x)$. 于是还得 $\Pi p_j = \Pi p_j'$. 由引理 3 知，$q_i(x)$ 及 $q_i'(x)$ 在 $\mathfrak{F}[x]$ 里是不可約的．因为 $\mathfrak{F}[x]$是高斯整区，故 $q_i'(x)$ 可予以改編，使 $q_i'(x)$ 是 $q_i(x)$ 在 $\mathfrak{F}[x]$ 里的一个相伴元素．但引理 1 指出，这些多项式在 $\mathfrak{A}[x]$ 里也是相伴的．末了，因为 $\mathfrak{A}$ 是高斯整区，因子分解 $\Pi p_i = \Pi p_i'$ 里的素元素 p_i 及 p_i' 可搭配成一对对相伴元素．于是，(4)里两种因子分解实質上是相同的．

这定理的一个直接推論是：如果 $\mathfrak{A}$ 是高斯整区，而 x_i 是代数无关元素，則 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ 是高斯整区．例如，如果 $\mathfrak{F}$ 是任一个域，則 $\mathfrak{F}[x_1, x_2, \cdots, x_r]$ 是高斯整区．$I[x_1, x_2, \cdots, x_r]$ 也是高斯整区．但当 $r > 1$ 时的环 $\mathfrak{F}[x_1, x_2, \cdots, x_r]$ 及 $r \geqslant 1$ 时的环 $I[x_1, x_2, \cdots, x_r]$ 都不是主理想环．故高斯整区的范围远比主理想整区的范围大．

习　題　50

1. 如果 $f(x) \in I[x]$，它的首項系数是 1，并且它有一个有理根．求証：这个根是整数．

2. 求証下面的爱森斯坦 (Eisenstein) 不可約性判别准則：如果 $f(x) = a_0 + a_1x + \cdots + a_nx^n \in I[x]$，并且存在有素数 $p \in I$ 使 $p|a_0, p|a_1, \cdots, p|a_{n-1}$，但 $p \nmid a_n$ (p 不是 a_n 的因子)，而且 $p^2 \nmid a_0$，則$f(x)$ 在 $I[x]$ 里不可約，从而在 $R_0[x]$里也是不可約，这里 R_0 是有理数域．

3. 如果 p 是一个素数，驗証：以 $x+1$ 代替
$$x^{p-1} + x^{p-2} + \cdots + 1 = (x^p - 1)/(x - 1)$$
里的 x 所得的多項式在 $R_0[x]$ 里是不可約的．由此証明：割圓多項式 $x^{p-1} + x^{p-2} + \cdots + 1$ 在 $R_0[x]$ 里是不可約的．

第 五 章

带 算 子 群

本章継續羣論的探討．我們所得的結果涉及一个羣的子羣与它們的同态象間的对应、正規羣列及合成羣列、叔萊尔(Schreier)定理、直接积及克魯尔-叔密特(Krull-Schmidt)定理．这些結果的应用范围随着带算子羣的新概念的导入而大为扩张．这个概念首經克魯尔及諾德(Emmy Noether)研究，使我們能够探討与任意自同态的集合相关的一个羣．这样就使前此各別导出的若干古典結果得到統一的推理．又由以乘法映照的集合作为算子区而考究与它相关的加法羣，得出在环論上的应用．

1. 带算子羣的定义及例

定义 1. 带算子羣是由一个羣 $\mathfrak{G}$、一个集合 M 及定义在积集合 $\mathfrak{G}\times M$ 里而值在 $\mathfrak{G}$ 里的一个函数所組成的代数系，如果 am 表示由 $\mathfrak{G}$ 的元素 a 与 M 的元素 m 所决定的 $\mathfrak{G}$ 里元素，則对于 $\mathfrak{G}$ 里的 a,b 都有

(1) $$(ab)m=(am)(bm).$$

如果 m 固定，而 x 在 $\mathfrak{G}$ 上变，則 $x\rightarrow xm$ 是 $\mathfrak{G}$ 到它自身上一个映照，記做 $\bar{m}$．由假設(1)知 $\bar{m}$ 是 $\mathfrak{G}$ 里一个自同态．所以，每个元素 $m\in M$ 决定一个自同态 $\bar{m}$，并且得出 m 到 $\mathfrak{G}$ 的自同态的集合 $\mathfrak{E}$ 內的一个映照 $m\rightarrow\bar{m}$．这种映照不必是 1—1 的，亦卽 m 与 n 在 M 里不相同时，可能有 $\bar{m}=\bar{n}$．根据这些說明，我們得到带算子羣的概念的另一个定义如次：

定义 1′. 带算子羣是由一个羣 $\mathfrak{G}$、一个集合 M 及 M 到 $\mathfrak{G}$ 的自同态的集合內的一个映照 $m\rightarrow\bar{m}$ 所組成的代数系．

我們知道，如果 $\mathfrak{G}$, M 及映照 $(a,m)\rightarrow am$ 按定义 1 的意义成

一个带算子羣,則 $x \to xm$ 是 $\mathfrak{G}$ 里一个自同态. 我們还得出对应 $m \to \bar{m}$. 故得适合定义 1′ 的一个代数系. 反过来, 如果我們有按定义 1′ 的一个代数系,則可定义出映照 $(a,m) \to am = a\bar{m}$, 并且知道 (1) 能成立. 于是,得出适合定义 1 的一个带算子羣. 最后,如果我們从适合 1(1′)的一个代数系开始,接連使用变一种代数系为他种代数系的两个方法, 显然又回到原来代数系. 故两个定义等价.

第二个定义較适宜于作出带算子羣的例子. 为着这个目的,我們可取羣 $\mathfrak{G}$ 的自同态的任意一个集合为 M,并可令映照 $m \to \bar{m}$ 是恆等映照. 在这方面可使用的重要自同态的集合是:(1)內自同构集合 $\mathfrak{I}$,(2) 自同构的全集合 $\mathfrak{A}$,(3)自同态的集合 $\mathfrak{E}$.

用第一个定义較方便决定的一个例子为: $\mathfrak{G}$ 是三維空間里的向量羣,M是实数的集合,积函数 vt 是通常的数与向量的积,这里 $v \in \mathfrak{G}, t \in M$. 所以,如果 $v = (x,y,z)$, 則

$$vt = (tx,ty,tz).$$

我們熟知的法則

$$(v + v')t = vt + v't$$

是(1)在加法的形式.

带算子羣的理論在环論上也有重要的应用. 这些应用是由考究在环的加法羣里定义某些带算子羣而产生. 这样带算子羣有三种. 在这三种里, 羣 $\mathfrak{G}$ 总是取加法羣 $\mathfrak{A},+$, M 取 $\mathfrak{A},+$ 的自同态的集合, 而M的映照是恆等映照. 第一种取 M 为右乘变换的集合 $\mathfrak{A}_r$, 第二种取 M 为左乘变换的集合 $\mathfrak{A}_l$, 第三种取 $M = \mathfrak{A}_r \cup \mathfrak{A}_l$. 我們分別說: $\mathfrak{A}$ 在它的加法羣里作用于右,于左,或于双侧.

我們常是用語句"$\mathfrak{G}$ 是带算子集合M的羣",或"$\mathfrak{G}$ 是一个M-羣"来指陈一个带算子羣.

应用 $\bar{m}$ 是一个自同态这一事实可导出积 am 的若干初等性質. 譬如, 显然地有 $1m = 1$, $a^{-1}m = (am)^{-1}$, 以及更一般地对

于任一个整数 $k, a^k m = (am)^k$.

2. M-子羣, M-商羣及 M-同态 我們闡述带算子羣的概念重点放在一些子羣的集合上，这些子羣經由自同态的一个特殊集合映照到它們自身內；这因为，在討論一个 M-羣时，自然地把注意力限于 $\mathfrak{G}$ 的这些子羣上. 如果 $\mathfrak{H}$ 是一个子羣，且对于每个 $h \in \mathfrak{H}$ 及 $m \in M$ 必有 $hm \in \mathfrak{H}$，則說 $\mathfrak{H}$ 是一个 M-子羣.

来了解前节的例子里那些为 M-子羣是有趣味的. 在(1)里，$M = \mathfrak{I}$，則 $\mathfrak{H}$ 是一个 M-子羣必須而且只須对于各个 $g \in \mathfrak{G}, g^{-1}\mathfrak{H}g \subseteq \mathfrak{H}$ 成立，故 M-子羣恰是 $\mathfrak{G}$ 的不变子羣. 在(2)里，$M = \mathfrak{A}$，則 M-子羣 $\mathfrak{H}$ 特别是不变子羣. 而且对于 $\mathfrak{G}$ 的每个自同构都把 $\mathfrak{H}$ 映到它自身內. 具有这种性質的子羣叫做特征子羣. 在(3)里，$M = \mathfrak{E}$，此时 $\mathfrak{H}$ 是一个 M-子羣必須而且只須 $\mathfrak{H}$ 对于 $\mathfrak{G}$ 的每个自同态都把它映到自身內. 具有这种性質的子羣叫做全不变子羣. 在向量羣的例子里，如果一个子羣 $\mathfrak{H}$ 对于純量乘法封閉，則 $\mathfrak{H}$ 是一个 M-子羣. 这样子羣叫做子空間.

我們还考究由环决定的带算子羣. 如果 $\mathfrak{A}$ 作用于右 ($M = \mathfrak{A}_r$)，則子集合 $\mathfrak{B}$ 是一个 M-子羣必須而且只須它是加法羣 $\mathfrak{A}, +$ 的一个子羣，并且对于 $\mathfrak{A}$ 的任意元素的右乘变換封閉. 故此时的 M-子羣是环的各个右理想. 同理，如果 $\mathfrak{A}$ 作用于左，則 M-子羣是环的各个左理想. 最后，如果 $\mathfrak{A}$ 作用于双側，則 M-子羣是各个双側理想.

如果 $\{\mathfrak{H}\}$ 是 $\mathfrak{G}$ 的 M-子羣的集合，这些羣的交 $\cap\mathfrak{H}$ 显然是一个 M-子羣. 由这些子羣生成的羣 $\mathfrak{S} = [\cup\mathfrak{H}]$ 也是一个 M-子羣；这因为，这个羣的元素是有限积 $h = h_1h_2\cdots h_n$, $h_i \in \mathfrak{H}_i \in \{\mathfrak{H}\}$. 因为 $h_i m \in \mathfrak{H}_i$，故 $hm = (h_1m)(h_2m)\cdots(h_nm) \in \mathfrak{S}$.

如果 $\mathfrak{H}$ 是 M-羣 $\mathfrak{G}$ 的一个 M-子羣，則 $\mathfrak{H}$ 可認为也是一个 M-羣，这里积 hm, $h \in \mathfrak{H}$, $m \in M$ 是按 M-羣 $\mathfrak{G}$ 里求积的法則来定义的. 故(1)显然成立. 今将驗証：如果 $\mathfrak{H}$ 是不变子羣，則商羣 $\bar{\mathfrak{G}} = \mathfrak{G}/\mathfrak{H}$ 也可以自然地認为是一个 M-羣，只要对于各个 $g \in \mathfrak{G}$ 及 $m \in M$，規定

(2) $$(g\mathfrak{H})m=(gm)\mathfrak{H}.$$

必須指出，这样规定的积是单值的，并且 (1) 成立. 这因为，令 $g\mathfrak{H}=g'\mathfrak{H}$,則 $g'=gh, h\in\mathfrak{H}$,而且 $g'm=(gm)(hm)$,这里 $hm\in\mathfrak{H}$ 故 $(gm)\mathfrak{H}=(g'm)\mathfrak{H}$. 这証明了单值的說法. 又因为

$$\begin{aligned}((g_1\mathfrak{H})(g_2\mathfrak{H}))m&=(g_1g_2\mathfrak{H})m=((g_1g_2)m)\mathfrak{H}\\&=((g_1m)(g_2m))\mathfrak{H}=((g_1m)\mathfrak{H})((g_2m)\mathfrak{H})\\&=((g_1\mathfrak{H})m)((g_2\mathfrak{H})m).\end{aligned}$$

故(1)也成立. 这样定义的带算子羣叫做 M-商羣 $\mathfrak{G}/\mathfrak{H}$.

今就有相同的算子集合 M 来比較带算子羣. 我們要考究的基本概念是同态. 如果 $\mathfrak{G}$ 及 $\mathfrak{G}'$ 都是 M-羣,而 η 是 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 内的一个同态,并且对于所有 $a\in\mathfrak{G}$ 及 $m\in M$,

(3) $$(am)\eta=(a\eta)m$$

成立,則 η 叫做一个同态 (M-同态). 我們也可得出同态的通常各特款:如果 η 是 1—1 的,就叫做同构;如果 $\mathfrak{G}'=\mathfrak{G}$,就叫做自同态;如果 $\mathfrak{G}'=\mathfrak{G}$, 并且 η 是 $\mathfrak{G}$ 到它自身上的 1—1 映照,就叫做自同构. 如果有 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 上的一个同构存在,則說它們是同构的，記作 $\mathfrak{G}\cong\mathfrak{G}'$.

如果 η 是 $\mathfrak{G}$ 的一个自同态,則条件(3)与条件 $\bar{m}\eta=\eta\bar{m}$ 等价. 故 M-自同态是能与自同态 $\bar{m}$ 交換的各个自同态.

今令 η 是 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 内的一个 M-同态, 并令 $a\eta$ 是象集合 $\mathfrak{G}\eta$ 的任一个元素. 如果 $m\in M$, 則 $(a\eta)m=(am)\eta\in\mathfrak{G}\eta$. 因为 $\mathfrak{G}\eta$ 是一个子羣,这指出 $\mathfrak{G}\eta$ 是 $\mathfrak{G}'$ 的一个 M-子羣. 其次,我們考究 η 的核 $\mathfrak{K}$, 則知 $\mathfrak{K}$ 是 $\mathfrak{G}$ 的一个不变子羣. 如果 $k\in\mathfrak{K}$, 并且 $m\in M$, 則还有

$$(km)\eta=(k\eta)m=1'm=1'.$$

故 $km\in\mathfrak{K}$, 而 $\mathfrak{K}$ 是 $\mathfrak{G}$ 的一个 M-子羣. 故得:

定理 1. 如果 η 是 M-羣 $\mathfrak{G}$ 到 M-羣 $\mathfrak{G}'$ 内的一个同态,則像 $\mathfrak{G}\eta$ 是 $\mathfrak{G}'$ 的一个 M-子羣, 並且同态核是 $\mathfrak{G}$ 的一个不变 M-子羣.

习 题 51

1. 求証：$\mathfrak{G}$ 的特征(全不变)子羣 $\mathfrak{H}$ 的任一个特征 (全不变) 子羣 $\mathfrak{K}$ 是 $\mathfrak{G}$ 的特征(全不变)子羣.

2. 求証：循环羣的任一个子羣是全不变的.

3. 求証：由所有换位子 $[s,t]\equiv sts^{-1}t^{-1}$ 生成的子羣 $\mathfrak{G}^{(1)}$ 是一个全不变子羣，这里 $s,t\in\mathfrak{G}$. $\mathfrak{G}^{(1)}$ 叫做 $\mathfrak{G}$ 的 (第一)换位子子羣. 証明：$\mathfrak{G}/\mathfrak{G}^{(1)}$ 是交换羣，并且如果 $\mathfrak{H}$ 是任一个不变子羣能使 $\mathfrak{G}/\mathfrak{H}$ 是交换羣时，則 $\mathfrak{H}\supseteq\mathfrak{G}^{(1)}$.

4. 令 $\mathfrak{A}$ 是带恆等元素环，并取 $M=\mathfrak{A}_r$，而把 $\mathfrak{A}$ 看作一个 M-羣. 間 $\mathfrak{A}$ 的 M-自同态是什么？如果取 $M=\mathfrak{A}_r\cup\mathfrak{A}_l$，則 $\mathfrak{A}$ 的 M-自同态是什么？

3. 关于 M-羣的同态基本定理 M-同态的积显然是一个 M-同态. 如果 $\mathfrak{H}$ 是 M-羣 $\mathfrak{G}$ 的不变 M-子羣，則 $\mathfrak{G}$ 到 M-羣 $\bar{\mathfrak{G}}=\mathfrak{G}/\mathfrak{H}$ 上的自然映照 ν 也是一个 M-同态；这因为，由定义，$(g\mathfrak{H})m=(gm)\mathfrak{H}$，并且因为 $g\nu=g\mathfrak{H}$，故得 $g\nu m=gm\nu$.

次令 η 为 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 內的一个 M-同态，并令 $\mathfrak{H}$ 是 $\mathfrak{G}$ 的一个不变 M-子羣，含于 η 的核 $\mathfrak{K}$ 里，則与普通羣的情形(参看 §16) 相同，$g\mathfrak{H}\to g\eta$ 是单值对应，并且它决定由 M-羣 $\bar{\mathfrak{G}}=\mathfrak{G}/\mathfrak{H}$ 到 $\mathfrak{G}'$ 內的一个同态 $\bar{\eta}$. 唯一要証明的新事实是：$\bar{\eta}$ 关于 M 里元素也能很好地处理，亦即 $((g\mathfrak{H})m)\bar{\eta}=((g\mathfrak{H})\bar{\eta})m$. 这可由

$$((g\mathfrak{H})m)\bar{\eta}=((gm)\mathfrak{H})\bar{\eta}=(gm)\eta=(g\eta)m=((g\mathfrak{H})\bar{\eta})m,$$

知其为眞. 我們也可得因子分解 $\eta=\nu\bar{\eta}$，这里 ν 是 $\mathfrak{G}$ 到 $\bar{\mathfrak{G}}$ 上的自然映照. 又 $\bar{\eta}$ 是 1—1 的必須而且只須 $\mathfrak{K}=\mathfrak{H}$. 故得

关于 M-羣的同态基本定理 $\mathfrak{G}$ 关于一个不变 M-子群的商群是 $\mathfrak{G}$ 的一个同态像. 反过来，如果 $\mathfrak{G}'$ 是一个 M-群，而且是 M-群 $\mathfrak{G}$ 的一个同态像，則 $\mathfrak{G}'$ 必与 $\mathfrak{G}$ 关于一个不变 M-子群的商群是同構的.

4. 由一个同态决定的 M-子羣間的对应 上面只是把前此关于普通羣的結果扩张到 M-羣，今将导出一些新結果. 必須指出，当 M 是空集合时，則 M-子羣变为普通子羣，M-同态变为普通同态等等，故普通羣的理論是 M-羣理論的特殊情形. 因此新結果也可应用于普通羣.

令 η 是 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 上的一个 M-同态，并令 $\mathfrak{K}$ 是它的核. 如果

$\mathfrak{H}$ 是 $\mathfrak{G}$ 的一个 M-子羣，則 η 把 $\mathfrak{H}$ 同态地映到 $\mathfrak{G}'$ 的 M-子羣 $\mathfrak{H}\eta$ 上. 反过来，如果 $\mathfrak{H}'$ 是 $\mathfrak{G}'$ 的任一个 M-子羣，則逆象 $\mathfrak{H}=\eta^{-1}(\mathfrak{H}')$ 是 $\mathfrak{G}$ 的一个 M-子羣. 这因为，如果 $h_1,h_2\in\mathfrak{H}$，則 $(h_1h_2^{-1})\eta=(h_1\eta)(h_2\eta)^{-1}\in\mathfrak{H}'$，故 $h_1h_2^{-1}\in\mathfrak{H}$. 再則，如果 $h\in\mathfrak{H}$，$m\in M$，則 $(hm)\eta=(h\eta)m\in\mathfrak{H}'$. 故 $hm\in\mathfrak{H}$.

$\mathfrak{H}=\eta^{-1}(\mathfrak{H}')$ 显然包含 $\mathfrak{K}=\eta^{-1}(1')$，并且 $\mathfrak{H}\eta=\mathfrak{H}'$. 故知，如果把 η 使用于 $\mathfrak{G}$ 里包含着 $\mathfrak{K}$ 的 M-子羣，就可得出 $\mathfrak{G}'$ 的各个 M-子羣. 今令 $\mathfrak{H}$ 是 $\mathfrak{G}$ 里包含着 $\mathfrak{K}$ 的任一个 M-子羣，并令 $\mathfrak{H}_1=\eta^{-1}(\mathfrak{H}\eta)$. 显然，$\mathfrak{H}_1\supseteq\mathfrak{H}$. 反过来，如果 $h_1\in\mathfrak{H}_1$，則 $\mathfrak{H}$ 里必有某些 h 使 $h_1\eta=h\eta$. 于是，$h_1=hk$，$k\in\mathfrak{K}$. 因为 $\mathfrak{H}\supseteq\mathfrak{K}$，故得 $h_1\in\mathfrak{H}$. 于是，$\eta^{-1}(\mathfrak{H}\eta)=\mathfrak{H}$.

至此，容易証明下面的定理.

定理 2. 令 η 是 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 上的一个 M-同态，它的核是 $\mathfrak{K}$，并令 $\{\mathfrak{H}\}$ 是 $\mathfrak{G}$ 里包含着 $\mathfrak{K}$ 的 M-子群的集合，則 $\mathfrak{H}\to\mathfrak{H}\eta$ 是 $\{\mathfrak{H}\}$ 到 $\mathfrak{G}'$ 的 M-子群的集合上的1—1 映照，$\mathfrak{H}$ 是 $\mathfrak{G}$ 的不变子群必須而且只須它的像 $\mathfrak{H}'=\mathfrak{H}\eta$ 是 $\mathfrak{G}'$ 的不变子群.

証 我們知道，$\mathfrak{H}\to\mathfrak{H}\eta$ 是 $\{\mathfrak{H}\}$ 到 $\mathfrak{G}'$ 的 M-子羣的集合上的一个映照. 再則，如果 $\mathfrak{H}_1$ 及 $\mathfrak{H}_2\in\{\mathfrak{H}\}$，并且 $\mathfrak{H}_1\eta=\mathfrak{H}_2\eta$，則

$$\mathfrak{H}_1=\eta^{-1}(\mathfrak{H}_1\eta)=\eta^{-1}(\mathfrak{H}_2\eta)=\mathfrak{H}_2.$$

故这个映照是 1—1 的. 至于 $\mathfrak{H}$ 是 $\mathfrak{G}$ 里不变子羣必須而且只須 $\mathfrak{H}'=\mathfrak{H}\eta$ 是 $\mathfrak{G}'$ 的不变子羣；因为容易驗証，就不多贅述了.

这定理的一个重要特殊情形是考究 $\mathfrak{G}$ 到一个 M-商羣 $\mathfrak{G}/\mathfrak{K}$ 上的自然同态 ν，这里 $\mathfrak{K}$ 是一个不变 M-子羣. 此时，我們知道，$\bar{\mathfrak{G}}=\mathfrak{G}/\mathfrak{K}$ 的任一个 M-子羣可由使用 ν 于 $\mathfrak{G}$ 里包含着 $\mathfrak{K}$ 的一个 M-子羣 $\mathfrak{H}$ 而得出. 同态象 $\mathfrak{H}\nu$ 是陪集 $h\mathfrak{K}$ 的集合，这里 $h\in\mathfrak{H}$；故恰好是商羣 $\mathfrak{H}/\mathfrak{K}$. 因此可述成下面的系：

系. 令 $\mathfrak{G}$ 是一个 M-群，而 $\mathfrak{K}$ 是一个不变 M-子羣，則 M-商羣 $\mathfrak{G}/\mathfrak{K}$ 的任一个 M-子羣的形狀为 $\mathfrak{H}/\mathfrak{K}$，这里 $\mathfrak{H}$ 是 $\mathfrak{G}$ 里包含着 $\mathfrak{K}$ 的一个 M-子羣. 不同的 $\mathfrak{H}$ 按这方法生成 $\mathfrak{G}/\mathfrak{K}$ 里不同的 M-子羣，并且 $\mathfrak{H}$ 是 $\mathfrak{G}$ 的不变子羣必須而且只須 $\mathfrak{H}/\mathfrak{K}$ 是 $\mathfrak{G}/\mathfrak{K}$ 的

不变子羣.

环方面也有类似的結果，这可由直接証明或作为羣的定理的特款而得出，这里采取后一个方法. 令 η 是环 $\mathfrak{A}$ 到环 $\mathfrak{A}'$ 上的一个同态，并令 $\mathfrak{K}$ 是 η 的核. 則可把 $\mathfrak{A},+$ 看作带算子集合 $M=\mathfrak{A}_r\cup\mathfrak{A}_l$ 的一个羣. 再則，我們还可把 $\mathfrak{A}',+$ 看作一个M-羣，这因为，我們可定义

$$(4)\qquad \begin{aligned} x'a_r &\equiv x'(a\eta)_r = x'(a\eta),\\ x'a_l &\equiv x'(a\eta)_l = (a\eta)x'. \end{aligned}$$

这样的定义显然满足(1)的基本要求的；这因为，当我們使用这个定义时，由于

$$\begin{aligned} (x\eta)a_r &= (x\eta)(a\eta) = (xa)\eta = (xa_r)\eta,\\ (x\eta)a_l &= (a\eta)(x\eta) = (ax)\eta = (xa_l)\eta, \end{aligned}$$

故 η 变为 $\mathfrak{A},+$ 到 $\mathfrak{A}',+$ 上的一个 M-同态. 最后必須指出，$\mathfrak{A}',+$ 的 M-子羣的确是环 $\mathfrak{A}'$ 的(双側)理想；这因为，如果 $\mathfrak{B}'$ 是一个 M-子羣，則对于 $\mathfrak{B}'$ 里各个 b' 有 $b'(a\eta)$ 及 $(a\eta)b'\in\mathfrak{B}'$. 因为集合 $\{a\eta\}=\mathfrak{A}'$，故 $\mathfrak{B}'$是一个理想. 逆定理显然也是眞的. 今定理 2 建立了 $\mathfrak{A}$ 里包含着 $\mathfrak{K}$ 的各理想的集合 $\{\mathfrak{B}\}$ 与 $\mathfrak{A}'$ 里理想的全体之間的一个1—1对应，故在特款就得出理想的集合$\{\mathfrak{B}\}$(这里 $\mathfrak{B}\supseteq\mathfrak{K}$) 与差环 $\mathfrak{A}/\mathfrak{K}$ 的各理想之間的一个1—1对应. 当 $\mathfrak{B}$ 是$\mathfrak{A}$里包含着 $\mathfrak{K}$ 的一个理想时，$\mathfrak{A}/\mathfrak{K}$ 的任一个理想的形状为 $\mathfrak{B}/\mathfrak{K}$. 而不同的 $\mathfrak{B}$生成不同的理想$\mathfrak{B}/\mathfrak{K}$.

习　题 52

1. 决定 $I/(m)$ $(m>0)$ 的理想.
2. 試直接导出一个环的理想与这个环的一个同态象的理想之間的对应.

5. 关于 M-羣的同构定理　本节将証明关于 M-羣的同构的三个重要定理. 其中的第一个可看做是:在一个羣的子羣与这个羣的同态象的子羣間建立对应的定理的补充. 与前一样，令 η 是M-羣 $\mathfrak{G}$ 到M-羣 $\mathfrak{G}'$ 上的一个同态，并令 $\mathfrak{K}$ 是核. 令 $\mathfrak{H}$ 是 $\mathfrak{G}$ 里包含着核 $\mathfrak{K}$ 的一个不变 M-子羣，并令 $\mathfrak{H}'=\mathfrak{H}\eta$. 如果 ν'是$\mathfrak{G}'$到$\mathfrak{G}'/\mathfrak{H}'$ 上的

一个自然同态，则 $\eta\nu'$ 是 $\mathfrak{G}$ 到 $\mathfrak{G}'/\mathfrak{H}'$ 上的一个同态。如果 $g\eta\nu'=\mathfrak{H}'$，则 $g\eta\in\mathfrak{H}'$；其逆亦真。故 $\eta\nu'$ 的核是羣 $\mathfrak{H}$。从基本定理知，由 $g\mathfrak{H}\rightarrow g\eta\nu'=(g\eta)\mathfrak{H}'$ 定义的 $\overline{\eta\nu'}$ 是 $\mathfrak{G}/\mathfrak{H}$ 到 $\mathfrak{G}'/\mathfrak{H}$ 上的一个 M-同构。这証明了

第一同构定理 令 η 是 M-羣 $\mathfrak{G}$ 到 M-羣 $\mathfrak{G}'$ 上的一个同态，$\mathfrak{K}$ 为同态核，并令 $\mathfrak{H}$ 是 $\mathfrak{G}$ 里包含着 $\mathfrak{K}$ 的一个不变 M-子羣，则 $\mathfrak{H}\eta=\mathfrak{H}'$ 是 $\mathfrak{G}'$ 里不变子羣，而且 M-商羣 $\mathfrak{G}/\mathfrak{H}$ 与 $\mathfrak{G}'/\mathfrak{H}'$ 在对应 $g\mathfrak{H}\rightarrow(g\eta)\mathfrak{H}'$ 下是同構的。

这定理的一个特款是取 $\mathfrak{G}'$ 为 M-商羣 $\mathfrak{G}/\mathfrak{K}$，而 $\eta=\nu$ 是自然同态。如果 $\mathfrak{H}$ 是 $\mathfrak{G}$ 里包含着 $\mathfrak{K}$ 的一个不变 M-子羣，则 $\mathfrak{H}\eta$ 是陪集 $h\mathfrak{K}$ 組成的商羣 $\mathfrak{H}/\mathfrak{K}$，这里 $h\in\mathfrak{H}$。故得

系. 如果 $\mathfrak{K}$ 及 $\mathfrak{H}$ 是 $\mathfrak{G}$ 的不变 M-子羣，而 $\mathfrak{H}\supseteq\mathfrak{K}$，则 $\mathfrak{G}/\mathfrak{H}$ 与 $(\mathfrak{G}/\mathfrak{K})/(\mathfrak{H}/\mathfrak{K})$ 是同構的。

次設 $\mathfrak{G}_1$ 及 $\mathfrak{G}_2$ 是 $\mathfrak{G}$ 的 M-子羣，而 $\mathfrak{G}_2$ 是不变子羣，则由 $\mathfrak{G}_1$ 及 $\mathfrak{G}_2$ 生成的 M-子羣是积集合 $\mathfrak{G}_1\mathfrak{G}_2=\mathfrak{G}_2\mathfrak{G}_1$。$g_1\rightarrow g_1\mathfrak{G}_2(g_1\in\mathfrak{G}_1)$ 显然是 M-子羣 $\mathfrak{G}_1$ 到 $\mathfrak{G}_1\mathfrak{G}_2/\mathfrak{G}_2$ 内的一个同态。因为 $\mathfrak{G}_1\mathfrak{G}_2$ 里任一个陪集的形状为 $g_1g_2\mathfrak{G}_2=g_1\mathfrak{G}_2$，这里 $g_i\in\mathfrak{G}_i$。故上面的同态是 $\mathfrak{G}_1$ 到 $\mathfrak{G}_1\mathfrak{G}_2/\mathfrak{G}_2$ 上的一个映照。如果 $g_1\mathfrak{G}_2=\mathfrak{G}_2$，则 $g_1\in\mathfrak{G}_2$；因而 $g_1\in\mathfrak{G}_1\cap\mathfrak{G}_2$。这指出，同态 $g_1\rightarrow g_1\mathfrak{G}_2$ 的核是 $\mathfrak{G}_1\cap\mathfrak{G}_2$。故得下面的定理。

第二同构定理 如果 $\mathfrak{G}_1$ 及 $\mathfrak{G}_2$ 是一个羣的 M-子羣，并且 $\mathfrak{G}_2$ 是不变子羣，则(1) $\mathfrak{G}_1\cap\mathfrak{G}_2$ 是 $\mathfrak{G}_1$ 里的不变子羣，并且(2) M-子羣 $\mathfrak{G}_1\mathfrak{G}_2/\mathfrak{G}_2$ 与 $\mathfrak{G}_1/(\mathfrak{G}_1\cap\mathfrak{G}_2)$ 在对应 $g_1\mathfrak{G}_2\rightarrow g_1(\mathfrak{G}_1\cap\mathfrak{G}_2)$ 下是同構的。

我們还建立更复杂的同构定理；这定理将于下一节用来証明重要的叔莱尔加細定理。

第三同构定理（札森豪斯(Zassenhaus)定理） 令 $\mathfrak{G}_i'$ 及 $\mathfrak{G}_i(i=1,2)$ 是 $\mathfrak{G}$ 的 M-子羣，而 $\mathfrak{G}_i'$ 是 $\mathfrak{G}_i$ 的不变子羣，则 $(\mathfrak{G}_1\cap\mathfrak{G}_2')\mathfrak{G}_1'$ 是 $(\mathfrak{G}_1\cap\mathfrak{G}_2)\mathfrak{G}_1'$ 的不变子羣，$(\mathfrak{G}_1'\cap\mathfrak{G}_2)\mathfrak{G}_2'$ 是 $(\mathfrak{G}_1\cap\mathfrak{G}_2)\mathfrak{G}_2'$ 的不变子羣，并且它們的对应商羣是 M-同構的。

証 考究 $(\mathfrak{G}_1\cap\mathfrak{G}_2)\mathfrak{G}_1'$ 的子羣 $(\mathfrak{G}_1\cap\mathfrak{G}_2')\mathfrak{G}_1'$。首先我們来直接地証明它是不变子羣。令 $x\in\mathfrak{G}_1\cap\mathfrak{G}_2$；$y\in\mathfrak{G}_1\cap\mathfrak{G}_2'$；$z,t\in\mathfrak{G}_1'$。则

$x^{-1}yx \in \mathfrak{G}_1 \cap \mathfrak{G}_2'$，而 $x^{-1}zx \in \mathfrak{G}_1'$，故

(5) $$x^{-1}(\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1'x \subseteq (\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1'.$$

因为 $t^{-1}yt = y(y^{-1}t^{-1}y)t = y(y^{-1}ty)^{-1}t$，并且 $y^{-1}ty \in \mathfrak{G}_1'$，故 $(y^{-1}ty)^{-1}t \in \mathfrak{G}_1'$，而 $t^{-1}yt \in (\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1'$. 于是，

(6) $$t^{-1}(\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1't = t^{-1}(\mathfrak{G}_1 \cap \mathfrak{G}_2')tt^{-1}\mathfrak{G}_1't \subseteq (\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1'.$$

由(5)及(6)显然知，$(\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1'$ 是 $(\mathfrak{G}_1 \cap \mathfrak{G}_2)\mathfrak{G}_1'$ 的不变子羣. 由第二同构定理知，$(\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1' \cap (\mathfrak{G}_1 \cap \mathfrak{G}_2)$ 是 $\mathfrak{G}_1 \cap \mathfrak{G}_2$ 的不变子羣，并且

(7) $$\begin{aligned}(\mathfrak{G}_1 \cap \mathfrak{G}_2)/(\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1' \cap (\mathfrak{G}_1 \cap \mathfrak{G}_2) &\cong (\mathfrak{G}_1 \cap \mathfrak{G}_2)(\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1'/(\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1' \\ &= (\mathfrak{G}_1 \cap \mathfrak{G}_2)\mathfrak{G}_1'/(\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1'.\end{aligned}$$

另一方面，

(8) $$(\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1' \cap (\mathfrak{G}_1 \cap \mathfrak{G}_2) = (\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1' \cap \mathfrak{G}_2,$$

并且 $(\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1'$ 的任一个元素的形状是 yz，这里 $y \in \mathfrak{G}_1 \cap \mathfrak{G}_2'$，$z \in \mathfrak{G}_1'$. 如果 $yz \in \mathfrak{G}_2$，则 $z = y^{-1}(yz) \in \mathfrak{G}_2$，故 $z \in \mathfrak{G}_2 \cap \mathfrak{G}_1'$，于是，$yz \in (\mathfrak{G}_1 \cap \mathfrak{G}_2')(\mathfrak{G}_1' \cap \mathfrak{G}_2)$，而得

$$(\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1' \cap \mathfrak{G}_2 \subseteq (\mathfrak{G}_1 \cap \mathfrak{G}_2')(\mathfrak{G}_1' \cap \mathfrak{G}_2).$$

次令 $y \in \mathfrak{G}_1 \cap \mathfrak{G}_2'$，$z \in \mathfrak{G}_1' \cap \mathfrak{G}_2$，则 $y, z \in \mathfrak{G}_2$，从而 $yz \in \mathfrak{G}_2$；又由假設，$yz \in (\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1'$，故 $yz \in (\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1' \cap \mathfrak{G}_2$. 于是，又有

$$(\mathfrak{G}_1 \cap \mathfrak{G}_2')(\mathfrak{G}_1' \cap \mathfrak{G}_2) \subseteq (\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1' \cap \mathfrak{G}_2.$$

故知

$$(\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1' \cap \mathfrak{G}_2 = (\mathfrak{G}_1 \cap \mathfrak{G}_2')(\mathfrak{G}_1' \cap \mathfrak{G}_2).$$

因此，(7)可改写为

(9) $$(\mathfrak{G}_1 \cap \mathfrak{G}_2)/(\mathfrak{G}_1 \cap \mathfrak{G}_2')(\mathfrak{G}_1' \cap \mathfrak{G}_2) \cong (\mathfrak{G}_1 \cap \mathfrak{G}_2)\mathfrak{G}_1'/(\mathfrak{G}_1 \cap \mathfrak{G}_2')\mathfrak{G}_1'.$$

由对称性，还得

(10) $$(\mathfrak{G}_1 \cap \mathfrak{G}_2)/(\mathfrak{G}_1 \cap \mathfrak{G}_2')(\mathfrak{G}_1' \cap \mathfrak{G}_2) \cong (\mathfrak{G}_1 \cap \mathfrak{G}_2)\mathfrak{G}_2'/(\mathfrak{G}_1' \cap \mathfrak{G}_2)\mathfrak{G}_2'.$$

由(9)及(10)即得所求結果.

习　题 53

1. 求証：从第三同构定理可推得第二同构定理.

2. 令 $\mathfrak{G}_1, \mathfrak{G}_1'$ 是 M-子羣，而 $\mathfrak{G}_1'$ 是 $\mathfrak{G}_1$ 的一个不变子羣，并令 $\mathfrak{H}$ 是 $\mathfrak{G}$ 的任一个

M-子羣．求証：$\mathfrak{H}_1' = \mathfrak{G}_1' \cap \mathfrak{H}$ 是 $\mathfrak{H}_1 = \mathfrak{G}_1 \cap \mathfrak{H}$ 的不变子羣，并且 $\mathfrak{H}_1/\mathfrak{H}_1'$ 同构于 $\mathfrak{G}_1/\mathfrak{G}_1'$ 的一个子羣．

3．說出关于环上类似的第一及第二同构定理．

6. 叔萊尔定理 今考究一个羣分解为商羣的一种因子分解．令

(11) $$\mathfrak{G} = \mathfrak{G}_1 \supseteq \mathfrak{G}_2 \supseteq \cdots \supseteq \mathfrak{G}_{s+1} = 1$$

是 M-羣 $\mathfrak{G}$ 的 M-子羣的一个羣列，这里 $\mathfrak{G}_{i+1}$ 是 $\mathfrak{G}_i$ 的不变子羣．这样羣列叫做 $\mathfrak{G}$ 的正規羣列．商羣

(12) $$\mathfrak{G}_1/\mathfrak{G}_2, \mathfrak{G}_2/\mathfrak{G}_3, \cdots, \mathfrak{G}_s/\mathfrak{G}_{s+1} = \mathfrak{G}_s$$

是正規羣列的商．例如，令 $\mathfrak{G}$ 是 n 阶有限循环羣，則子羣 $\mathfrak{G}_i$ 由它的阶 n_i 来决定，并且 $n_{i+1}|n_i$．比 $q_i = n_i/n_{i+1}$ 是 $\mathfrak{G}_i/\mathfrak{G}_{i+1}$ 的阶．因为 $n = n_1 = q_1n_2$，$n_2 = q_2n_3, \cdots$，故 $n = q_1q_2\cdots q_s$．反过来，如果 $n = q_1q_2\cdots q_s$ 是 n 的一个因子分解，則循环羣 $\mathfrak{G}$ 有一个子羣 $\mathfrak{G}_i$，它的阶数 $n_i = q_iq_{i+1}\cdots q_s$．故 $\mathfrak{G} = \mathfrak{G}_1 \supseteq \mathfrak{G}_2 \supseteq \cdots \supseteq \mathfrak{G}_{s+1} = 1$，并且 $\mathfrak{G}_i/\mathfrak{G}_{i+1}$ 的阶数是 q_i．

如果在两个正規羣列

(13) $$\begin{aligned} \mathfrak{G} &= \mathfrak{G}_1 \supseteq \mathfrak{G}_2 \supseteq \cdots \supseteq \mathfrak{G}_{s+1} = 1, \\ \mathfrak{G} &= \mathfrak{H}_1 \supseteq \mathfrak{H}_2 \supseteq \cdots \supseteq \mathfrak{H}_{t+1} = 1 \end{aligned}$$

的商之間能建立一个 1—1 对应，使各对的商是同构的，則說这两个正規羣列是等价的．如果一个正規羣列的各項包含有出現在另一个正規羣列里的所有羣，則說前一个正規羣列是后一个正規羣列的一个加細．于是，可述下面的基本定理．

叔萊尔加細定理 一个 M-羣的任意两个正規羣列有等价的加細．

証 令这两个羣列是(13)，并令

(14) $$\begin{aligned} \mathfrak{G}_{ik} &= (\mathfrak{G}_i \cap \mathfrak{H}_k)\mathfrak{G}_{i+1}, \quad k = 1,2,\cdots,t+1, \\ \mathfrak{H}_{ki} &= (\mathfrak{G}_i \cap \mathfrak{H}_k)\mathfrak{H}_{k+1}, \quad i = 1,2,\cdots,s+1. \end{aligned}$$

則

$$\begin{aligned} \mathfrak{G} = \mathfrak{G}_{11} &\supseteq \mathfrak{G}_{12} \supseteq \cdots \supseteq \mathfrak{G}_{1,t+1} \\ &= \mathfrak{G}_{21} \supseteq \mathfrak{G}_{22} \supseteq \cdots \supseteq \mathfrak{G}_{2,t+1} \cdots \supseteq \mathfrak{G}_{s,t+1} = 1, \end{aligned}$$

(15)

$$\mathfrak{G} = \mathfrak{H}_{11} \supseteq \mathfrak{H}_{12} \supseteq \cdots \supseteq \mathfrak{H}_{1,s+1}$$
$$= \mathfrak{H}_{21} \supseteq \mathfrak{H}_{22} \supseteq \cdots \supseteq \mathfrak{H}_{2,s+1} \cdots \supseteq \mathfrak{H}_{t,s+1} = 1.$$

把第三同构定理应用于羣 $\mathfrak{G}_i$, $\mathfrak{H}_k$, $\mathfrak{G}_{i+1}$, $\mathfrak{H}_{k+1}$, 則得 $\mathfrak{G}_{i,k+1} = (\mathfrak{G}_i \cap \mathfrak{H}_{k+1})\mathfrak{G}_{i+1}$是 $\mathfrak{G}_{ik} = (\mathfrak{G}_i \cap \mathfrak{H}_k)\mathfrak{G}_{i+1}$ 的不变子羣, 而$\mathfrak{H}_{k,i+1} = (\mathfrak{G}_{i+1} \cap \mathfrak{H}_k)\mathfrak{H}_{k+1}$ 是 $\mathfrak{H}_{ki} = (\mathfrak{G}_i \cap \mathfrak{H}_k)\mathfrak{H}_{k+1}$ 的不变子羣, 并且 $\mathfrak{G}_{ik}/\mathfrak{G}_{i,k+1} \cong \mathfrak{H}_{ki}/\mathfrak{H}_{k,i+1}$. 故(15)的两个羣列都是正規羣列,且是等价的. 因为这两个羣列是(13)里两个羣列的加細,故定理完全証明.

习　题　54

1. 如果 $\mathfrak{G} = \mathfrak{G}_1 \supseteq \mathfrak{G}_2 \supseteq \cdots \supseteq \mathfrak{G}_{s+1} = 1$ 是 $\mathfrak{G}$ 的一个正规羣列,并且 $\mathfrak{H}$ 是任一个 M-子羣,求証:

$$\mathfrak{H} = (\mathfrak{H} \cap \mathfrak{G}_1) \supseteq (\mathfrak{H} \cap \mathfrak{G}_2) \supseteq \cdots \supseteq (\mathfrak{H} \cap \mathfrak{G}_{s+1}) = 1$$

是 $\mathfrak{H}$ 的一个正規羣列,并求証后者各个商同构于前者各个商的子羣.

2. 如果一个普通羣有一个正規羣列,它的各个商都是交换羣时,则这个普通羣叫做**可解羣**. 証明:一个可解羣的任一个子羣及任一个商羣都是可解的.

3. 毆归納地定义$\mathfrak{G}$的高阶导羣 $\mathfrak{G}^{(i)} = (\mathfrak{G}^{(i-1)})^{(1)}$(参看习題 51 第 3 題). 求証: $\mathfrak{G}$ 是可解羣,必須而且只須有整数 s 存在使 $\mathfrak{G}^{(s)} = 1$.

4. 求証:阶数是素数羃的任一个有限羣必为可解羣(参看习題 20 第 3 題).

7. 单純羣及約当-霍尔德(Jordan-Hölder)定理　任一个 M-羣 $\mathfrak{G}$ 中,子羣 $\mathfrak{G}$ 及 1 都是不变 M-子羣. 如果 $\mathfrak{G} \neq 1$,并且它的不变子羣只有它自身及1,則 $\mathfrak{G}$ 叫做 M-**单純羣**. 例如, 阶数为素数的任一个循环羣是单純羣. 另一类重要的单純羣可由下面的定理給出.

定理 3.　如果 $n \geqslant 5$, 則交代羣 A_n 是單純羣.

証　我們已知, A_n 可由它的三元循环 (ijk) 生成 (习題 14 第 2 題). 其次要指出的是: 如果 A_n 的一个不变子羣 $\mathfrak{H}$ 含有一个三元循环, 則它包含着所有三元循环; 因此就与 A_n 重合. 这因为,令$(123) \in \mathfrak{H}$,并令(ijk)是任一个三元循环,則可把映照 $1 \to i$, $2 \to j$, $3 \to k$ 扩张成 $1, 2, \cdots, n$ 的一个置換

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i & j & k & l & m & \cdots \end{pmatrix}.$$

如果 γ 是奇置换，则以 (lm) 右乘而得一个偶置换．故可假定 $\gamma\in A_n$．因为$\gamma^{-1}(123)\gamma=(ijk)\in\mathfrak{H}$，就得所要証的結果．今将指出：如果 $\mathfrak{H}\neq 1$，则 $\mathfrak{H}$ 必含有一个三元循环．令 α 是属于 $\mathfrak{H}$ 的一个置换，它 $\neq 1$，并且是 $\mathfrak{H}$ 里 $\neq 1$ 的置换中含有最多不变元素的置换．如果 α 不是一个三元循环，则 α 或是含有一个循环，它的长 $\geqslant 3$，从而受变动的元素超过三个；或且至少是两个不相交的对换的积．因此可假定

(16) $$\alpha=(123\cdots)(\ )\cdots,$$

或

(17) $$\alpha=(12)(34)\cdots.$$

因为 α 不是奇置換$(123k)$中的一个，故(16)里的 α 至少必变动其他两个数字，譬如説是4,5．今令 $\beta=(345)$，并作$\alpha_1=\beta^{-1}\alpha\beta$．如果 α 是(16)的形状，则

$$\alpha_1=(124\cdots)(\ )\cdots,$$

如果 α 是(17)的形状，则

$$\alpha_1=(12)(45)\cdots.$$

如果 α 使一个数字 $i>5$ 不变，则显然 α_1 也使它不变，从而 $\alpha_1\alpha^{-1}$ 也使它不变．但 α 取(16)的形状时，$1\alpha_1\alpha^{-1}=1$，而取(17)的形状时，$1\alpha_1\alpha^{-1}=1$，及 $2\alpha_1\alpha^{-1}=2$．故 $\alpha_1\alpha^{-1}$ 比 α 有更多的数字不变．因为 $\alpha_1\alpha^{-1}\neq 1$，这与 α 的选法矛盾．故 α 是一个三元循环，而定理完全証明．[1)]

如果 $\mathfrak{H}$ 是 $\mathfrak{G}$ 的不变M–子羣，$\mathfrak{G}\supset\mathfrak{H}$，并且不能有不变 M–子羣 $\mathfrak{K}$ 存在使 $\mathfrak{G}\supset\mathfrak{K}\supset\mathfrak{H}$，则 $\mathfrak{H}$ 叫做 $\mathfrak{G}$ 的**极大不变 M–子羣**．由一个羣的子羣与一个商羣的子羣之間的对应易知：**$\mathfrak{H}$ 是 $\mathfrak{G}$ 的极大不变M–子羣必須而且只須$\mathfrak{G}/\mathfrak{H}$是$M$–单純羣．**

設 $\mathfrak{G}$ 的正規羣列

(18) $$\mathfrak{G}=\mathfrak{G}_1\supset\mathfrak{G}_2\supset\cdots\supset\mathfrak{G}_{s+1}=1$$

中，每个 $\mathfrak{G}_{i+1}$ 都是 $\mathfrak{G}_i$ 的极大不变 M–子羣，则这个正規羣列叫做

1) 这个証明本質上与范德威尔登的近世代数上的証明相同．——著者注．

合成羣列. 所以合成羣列是一种正规羣列，它的各个商都是 $\neq 1$ 的单純羣. M-羣 $\mathfrak{G}$ 不一定都有一个合成羣列. 例如，如果 M 是空集合，而 $\mathfrak{G}$ 是一个无限交换羣，则 $\mathfrak{G}$ 沒有合成羣列. 要証明这事实，首先要指出的是：一个单純交换羣除 1 及整个羣外，沒有其他子羣，故这样的羣必須是素数阶的有限循环羣. 所以，如果(18)是普通交换羣的一个合成羣列，则商羣 $\mathfrak{G}_i/\mathfrak{G}_{i+1}$ 是素数阶的循环羣. 但若一个羣 $\mathfrak{G}$ 包含有限阶 m 的一个子羣 $\mathfrak{H}$ 及有限指数 r，则 $\mathfrak{G}$ 是有限阶 mr 的羣. 由此易知，如果一个羣具有一个合成羣列，它的商是有限羣，则它自身是有限羣. 特别是，$\mathfrak{G}$ 为一个普通交换羣，而有一个合成羣列时，则 $\mathfrak{G}$ 必是有限羣.

如果一个 M-羣有一个合成羣列，则合成商（= 合成羣列的商）是由羣唯一决定. 这就是下面定理的内容.

約当-霍尔德定理 一个 M-羣的任兩个合成羣列是等价的.

証 由叔萊尔定理知，合成群列有等价的加細. 反过来，由合成羣列的定义易知，这样羣列的加細与給定羣列有相同的 $\neq 1$ 的商. 因为在加細羣列的各商間成 1—1 对应，故等于 1 的商配成对；于是，$\neq 1$ 的商也配成对. 因为这些都是給定合成羣列的合成商，故知这两个合成羣列是等价的.

习 題 55

1. 应用約当-霍尔德定理于有限循环羣，以証明：一个正整数分解为正素数因子的唯一性.

2. 如果 $\mathfrak{G}$ 有一个合成羣列，求証：如果 $\mathfrak{G}$ 的任一个正規羣列里各項是眞遞減的，則可加細为一个合成羣列.

3. 如果 $\mathfrak{G}$ 有一个合成羣列，求証：$\mathfrak{G}$ 的任一个不变子羣及 $\mathfrak{G}$ 的任一个商羣各有一个合成羣列；并求証：这些羣列的合成商是 M-同构于 $\mathfrak{G}$ 的合成商.

8. 鏈条件 今叙述两个条件，它們一起成为 M-羣 $\mathfrak{G}$ 拥有合成羣列的充要条件.

I 降鏈条件. 如果

$$\mathfrak{G}_1 \supseteq \mathfrak{G}_2 \supseteq \mathfrak{G}_3 \supseteq \cdots$$

是 M-子羣的一个递降序列，使 $\mathfrak{G}_1$ 是 $\mathfrak{G}$ 的不变子羣，而每个 $\mathfrak{G}_{i+1}$

是 $\mathfrak{G}_i$ 的不变子羣时，则有正整数 N 存在，使 $\mathfrak{G}_N = \mathfrak{G}_{N+1} = \cdots$。

Ⅱ　升鏈条件. 如果 $\mathfrak{H}$ 是一个正規羣列的任一項，而

$$\mathfrak{H}_1 \subseteq \mathfrak{H}_2 \subseteq \mathfrak{H}_3 \subseteq \cdots$$

是 M-子羣的一个递升序列，都是 $\mathfrak{H}$ 的不变子羣，則有正整数 N 存在，使 $\mathfrak{H}_N = \mathfrak{H}_{N+1} = \cdots$.

我們知道，如果 $\mathfrak{G}$ 是交換羣，則任一个子羣都是不变的，并且任一个子羣必是一个正規羣列的一項. 此时，Ⅰ及Ⅱ可更簡单地叙述如次：

Ⅲ　如果

$$\mathfrak{G}_1 \supseteq \mathfrak{G}_2 \supseteq \mathfrak{G}_3 \supseteq \cdots$$

是 M-子羣的一个递降序列，則有正整数 N 存在，使 $\mathfrak{G}_N = \mathfrak{G}_{N+1} = \cdots$.

Ⅳ　如果

$$\mathfrak{H}_1 \subseteq \mathfrak{H}_2 \subseteq \mathfrak{H}_3 \subseteq \cdots$$

是 M-子羣的递升序列，則有正整数 N 存在，使 $\mathfrak{H}_N = \mathfrak{H}_{N+1} = \cdots$.

事实上，如果已知 $\overline{M} = \{\overline{m}\}$ 包含着 $\mathfrak{G}$ 的所有內自同构，則这两个条件也可用于非交換羣. 这因为，此时任一个 M-子羣也是不变的. 今証下面的

定理 4. 一个 M-羣 $\mathfrak{G}$ 有合成羣列的充要条件是 $\mathfrak{G}$ 适合这兩个鏈条件.

証　充分性. 首先我們要指出，如果 $\mathfrak{H} \neq 1$ 是一个正規羣列里一項，則 $\mathfrak{H}$ 含有一个极大不变 M-子羣. 这因为，或者 $\mathfrak{H}_1 = 1$ 是 $\mathfrak{H}$ 的极大不变子羣，或者存在有 $\mathfrak{H}$ 的一个眞不变 M-子羣 $\mathfrak{H}_2$，使 $\mathfrak{H}_1 \subset \mathfrak{H}_2$. 在后一个情形下，如果 $\mathfrak{H}_2$ 不是 $\mathfrak{H}$ 的一个极大不变 M-子羣，則有 $\mathfrak{H}$ 的一个眞不变 M-子羣 $\mathfrak{H}_3$ 存在，它眞的包含 $\mathfrak{H}_2$. 这样經过有限步驟后，必当停止；否則，就要得出 $\mathfrak{H}$ 的不变 M-子羣的一个无限眞递升序列，而与Ⅱ矛盾了. 既然証得一个正規羣列里任一項 $\mathfrak{H}$ 都有一个极大不变 M-子羣；在特款可知，$\mathfrak{G} = \mathfrak{G}_1$ 必含有一个极大不变 M-子羣 $\mathfrak{G}_2$，$\mathfrak{G}_2$ 也含有一个极大不变 M-子羣 $\mathfrak{G}_3$ 等等. 于是，得到眞递降序列 $\mathfrak{G} = \mathfrak{G}_1 \supset \mathfrak{G}_2 \supset \mathfrak{G}_3 \supset \cdots$，其中每个

$\mathfrak{G}_{i+1}$ 是前一个的极大不变 M-子羣. 由 I 知, 有一个有限数 $s+1$ 存在, 使 $\mathfrak{G}_{s+1}=1$. 故 $\mathfrak{G}$ 有一个合成羣列.

必要性. 令 $\mathfrak{G}$ 有一个合成羣列

$$\mathfrak{G}=\mathfrak{G}_1\supset\mathfrak{G}_2\supset\cdots\supset\mathfrak{G}_{s+1}=1,$$

并令 $\mathfrak{H}_1\supset\mathfrak{H}_2\supset\cdots$是 M-羣的一个眞递降序列, 使 $\mathfrak{H}_1$ 是 $\mathfrak{G}$ 的不变子羣, 而在 $i\geqslant 1$ 时, $\mathfrak{H}_{i+1}$是 $\mathfrak{H}_i$ 的不变子羣. 我們要証明: $\mathfrak{H}_i$ 的个数不会超过 $s+1$. 这因为, 如果超过 $s+1$, 則由于

$$\mathfrak{G}\supseteq\mathfrak{H}_1\supset\mathfrak{H}_2\supset\cdots\supset\mathfrak{H}_{s+2}\supseteq 1$$

是一个正規羣列, 故由叔莱尔定理知, 这个羣列存在一个加細, 使它与合成羣列的加細等价. 如果将重复的去掉后, 則得 $\mathfrak{H}$-羣列的一个加細, 它是一个合成羣列, 而其項数超过 $s+1$. 这与約当-霍尔德定理矛盾. 故 $\mathfrak{G}$ 必須适合 I. 同样論証知, $\mathfrak{G}$ 必須适合 II.

如果 $\mathfrak{G}$ 是一个有限羣, 显然 $\mathfrak{G}$ 对于任一个算子集合 M 适合鏈条件. 故对于任一个 M, 一个有限羣必有合成羣列. 当 M 为空集合时, 所得的一个合成羣列叫做常合成羣列. 这种羣列的形状为

$$\mathfrak{G}=\mathfrak{G}_1\supset\mathfrak{G}_2\supset\cdots\supset\mathfrak{G}_{s+1}=1,$$

这里 $\mathfrak{G}_{i+1}$ 是 $\mathfrak{G}_i$ 的一个不变子羣, 并且 $\mathfrak{G}_i/\mathfrak{G}_{i+1}$ 是一个单純羣. 約当-霍尔德定理証明由 $\mathfrak{G}$ 所决定的单純羣 $\mathfrak{G}_i/\mathfrak{G}_{i+1}$ 的集合的不变性. 如果 M 是內自同构的集合 $\mathfrak{J}$, 則 M-子羣是不变子羣, 此时合成羣列具有下面性質: 每个 $\mathfrak{G}_i$ 是 $\mathfrak{G}$ 的不变子羣, 并且 $\mathfrak{G}$ 里不存在不变子羣 $\mathfrak{G}'$ 使 $\mathfrak{G}_i\supset\mathfrak{G}'\supset\mathfrak{G}_{i+1}$. 这样的合成羣列叫做首要羣列. 仿此, 如果 M 是自同构的全集合, 此时的合成羣列叫做特征羣列. 如果 M 是自同态的全集合, 此时的合成羣列叫做全不变羣列. 对于这几种羣列, 約当-霍尔德定理当然也可应用.

习　題　56

1. 求 S_3 及 S_4 的合成群列.
2. 求証: 一个有限群是可解的必須而且只须它的合成商都是素数阶的循环羣.
3. 求証: 一个无限循环羣($M=\phi$)适合升鏈条件, 但不适合降鏈条件.
4. 令 $U_{(p)}$ 是 1 的 p^k 个复根的乘法羣, 这里 p 是固定的素数, 而 $k=0,1,2,3,\cdots$. 求証: $U_{(p)}$的各个眞子群是有限循环群. 于是, 求証: $U_{(p)}$ 适合降鏈条件, 但不适合升鏈条件.

9. 直接积 本节討論从 n 个給定的 M-羣 $\mathfrak{G}_1, \mathfrak{G}_2, \cdots, \mathfrak{G}_n$ 作出一个 M-羣的一个簡单作法. 令 $\mathfrak{G}$ 是积集合 $\mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_n$, 其元素为

$$a = (a_1, a_2, \cdots, a_n), a_i \in \mathfrak{G}_i,$$

并在 $\mathfrak{G}$ 里以公式

(19) $$(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n) = (a_1b_1, a_2b_2, \cdots, a_nb_n)$$

定义一个合成. 如果 $a = (a_i)$, $b = (b_i)$, 及 $c = (c_i)$, 則

$$(ab)c = ((a_ib_i)c_i) = (a_i(b_ic_i)) = a(bc).$$

元素

$$1 = (1, 1, \cdots, 1)$$

易知是 $\mathfrak{G}$ 里的恆等元素. 如果令 $a' = (a_i^{-1})$, 則 $aa' = 1 = a'a$. 故 $\mathfrak{G}$ 按上述的合成成一个羣. 其次, 对于 $m \in M$, 定义

(20) $$(a_1, a_2, \cdots, a_n)m = (a_1m, a_2m, \cdots, a_nm),$$

則

$$(ab)m = ((a_ib_i))m = ((a_ib_i)m) = ((a_im)(b_im))$$
$$= (am)(bm),$$

故 $\mathfrak{G}$ 是一个 M-羣. 这个 M-羣叫做 $\mathfrak{G}_i$ 的**直接积**, 記作

$$\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_n.$$

如果每个 $\mathfrak{G}_i$ 是 n_i 阶有限羣, 显然 $\mathfrak{G}$ 是 $n = \Pi n_i$ 阶有限羣. $\mathfrak{G}$ 是交換羣必須而且只須各个 $\mathfrak{G}_i$ 都是交換羣. 如果在羣 $\mathfrak{G}_i$ 里采用加法記号, 則可写成

(19′) $$(a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n)$$
$$= (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n)$$

以代替 (19), 此时 $\mathfrak{G}$ 叫做 $\mathfrak{G}_i$ 的**直接和**, 記作

$$\mathfrak{G} = \mathfrak{G}_1 \oplus \mathfrak{G}_2 \oplus \cdots \oplus \mathfrak{G}_n.$$

§1 里所給关于三維实向量羣的例实际上是直接和 $\mathfrak{G} \oplus \mathfrak{G} \oplus \mathfrak{G}$, 这里 $\mathfrak{G}$ 是关于实数的算子集合的实数加法羣, 而用普通乘法做运算. 这由定义就可明白的; 并且立刻可以推广到 n 維向量羣. 直接和的另一个重要例子是羣 $\mathfrak{G} \oplus \mathfrak{G} \oplus \cdots \oplus \mathfrak{G}$, 这里 $\mathfrak{G}$ 是整数的加法羣, 而 $M = \emptyset$. 这羣的元素是整数向量 (或"整点"), 而加法是

用通常的向量加法(19′).

今就任意羣的直接积作两点簡单説明．第一是直接积与商的次序无关；就是説，如果 $1',2',\cdots,n'$ 是 $1,2,\cdots,n$ 的一个置换，则 $\mathfrak{G}_{1'}\times\mathfrak{G}_{2'}\times\cdots\times\mathfrak{G}_{n'}$ M-同构于 $\mathfrak{G}_1\times\mathfrak{G}_2\times\cdots\times\mathfrak{G}_n$. 事实上，我們易知，对应

$$(a_1,a_2,\cdots,a_n)\rightarrow(a_{1'},a_{2'},\cdots,a_{n'})$$

是一个 M-同构．其次，如果 $n_1<n_2<\cdots<n_r=n$，则

$$(\mathfrak{G}_1\times\cdots\times\mathfrak{G}_{n_1})\times(\mathfrak{G}_{n_1+1}\times\cdots\times\mathfrak{G}_{n_2})\times\cdots\times(\mathfrak{G}_{n_{r-1}+1}\times\cdots\times\mathfrak{G}_{n_r})$$

M-同构于 $\mathfrak{G}_1\times\mathfrak{G}_2\times\cdots\times\mathfrak{G}_n$. 这里映照

$$(a_1,a_2,\cdots,a_n)\rightarrow((a_1,a_2,\cdots,a_{n_1}),(a_{n_1+1},\cdots,a_{n_2}),\cdots(a_{n_{r-1}+1},\cdots,a_{n_r}))$$

是一个同构．在特款，因为 $(\mathfrak{G}_1\times\mathfrak{G}_2)\times\mathfrak{G}_3$ 及 $\mathfrak{G}_1\times(\mathfrak{G}_2\times\mathfrak{G}_3)$ 都与 $\mathfrak{G}_1\times\mathfrak{G}_2\times\mathfrak{G}_3$ 等价，故它們也是等价的．所以在 M-同构来説，羣的直接乘法是可結合的，也是可交换的.

10. 子羣的直接积 今将决定一个 M-羣同构于一个直接积的条件．为着这个目的，我們进一步討論直接积 $\mathfrak{G}=\mathfrak{G}_1\times\mathfrak{G}_2\times\cdots\times\mathfrak{G}_n$. 令 $\mathfrak{G}_i'$ 是 $\mathfrak{G}$ 里形状如

$$a_i'=(1,1,\cdots,1,a_i,1,\cdots,1)$$

的元素的集合，这里 a_i 在第 i 个位置．显然，$\mathfrak{G}_i'$ 是 $\mathfrak{G}$ 的一个 M-子羣，在对应

$$a_i\rightarrow(1,\cdots,1,a_i,1,\cdots,1)$$

下同构于 $\mathfrak{G}_i$. 又因为

$$(c_1^{-1},c_2^{-1},\cdots,c_n^{-1})(1,\cdots,1,a_i,1,\cdots,1)(c_1,c_2,\cdots,c_n)=(1,\cdots,1,c_i^{-1}a_ic_i,1,\cdots,1),$$

故 $\mathfrak{G}_i'$ 是 $\mathfrak{G}$ 的不变子羣．其次是，$\mathfrak{G}$ 的一个任意元素 $(a_1,a_2,\cdots,a_n)$ 等于积 $a_1'a_2'\cdots a_n'$，这里 $a_i'\in\mathfrak{G}_i'$，故

(21) $$\mathfrak{G}=\mathfrak{G}_1'\mathfrak{G}_2'\cdots\mathfrak{G}_n'.$$

换句話説，$\mathfrak{G}$ 里包含着所有 $\mathfrak{G}_i'$ 的最小子羣是 $\mathfrak{G}$ 自身．最后，因为

$$\mathfrak{G}_1'\mathfrak{G}_2'\cdots\mathfrak{G}_{i-1}'\mathfrak{G}_{i+1}'\cdots\mathfrak{G}_n'$$

里任一个元素的形状是

$$(a_1, a_2, \cdots, a_{i-1}, 1, a_{i+1}, \cdots, a_n),$$

而 $\mathfrak{G}_i'$ 的任一个元素的形状是 $(1,\cdots,1,a_i,1,\cdots,1)$；所以，等式

$$(a_1, a_2, \cdots, a_{i-1}, 1, a_{i+1}, \cdots, a_n) = (1,\cdots,1,a_i,1,\cdots,1)$$

可推得 $a_j = 1$. 于是，$\mathfrak{G}_i'$ 与 $\mathfrak{G}_1'\cdots\mathfrak{G}_{i-1}'\mathfrak{G}_{i+1}'\cdots\mathfrak{G}_n'$ 的公共元素的所有支量 $a_j = 1$. 故知

(22) $$\mathfrak{G}_i' \cap \mathfrak{G}_1'\mathfrak{G}_2'\cdots\mathfrak{G}_{i-1}'\mathfrak{G}_{i+1}'\cdots\mathfrak{G}_n' = 1,\ i = 1,2,\cdots,n.$$

因此我們已証明了下面定理的必要性部分.

定理 5. 一个M-羣$\mathfrak{G}$同構于一个直接積 $\mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_n$ 的充要条件是：$\mathfrak{G}$ 含有与 $\mathfrak{G}_i$ 同構的不变M-子羣 $\mathfrak{G}_i'$，使(21)及(22)成立.

今証明这条件的充分性. 設 M-羣 $\mathfrak{G}$ 含有同构于 $\mathfrak{G}_i$ 的不变M-子羣 $\mathfrak{G}_i'$，且适合(21)及(22). 則由(21)知，$\mathfrak{G}$ 的任一个元素的形状为 $a_1'a_2'\cdots a_n'$，这里 $a_i' \in \mathfrak{G}_i'$. 令 $i \neq j$，并考究积 $a_i'a_j'(a_i')^{-1}(a_j')^{-1}$. 因为 $a_i'(a_j')(a_i')^{-1} \in \mathfrak{G}_j'$，故 $a_i'a_j'(a_i')^{-1}(a_j')^{-1} \in \mathfrak{G}_j'$. 又因为 $a_j'(a_i')^{-1}(a_j')^{-1} \in \mathfrak{G}_i'$，故 $a_i'a_j'(a_i')^{-1}(a_j')^{-1} \in \mathfrak{G}_i'$. 但由(22)知，$\mathfrak{G}_i' \cap \mathfrak{G}_j' = 1$，故 $a_i'a_j'(a_i')^{-1}(a_j')^{-1} = 1$，而

$$a_i'a_j' = a_j'a_i'.$$

这証明了：每个羣 $\mathfrak{G}_i'$ 的任一个元素可与不同的羣 $\mathfrak{G}_j'$ 的任一个元素交换. 由此可推得，如果 $a_i' \in \mathfrak{G}_i'$，$b_i' \in \mathfrak{G}_i'$，则

(23) $$(a_1'a_2'\cdots a_n')(b_1'b_2'\cdots b_n') = (a_1'b_1')(a_2'b_2')\cdots(a_n'b_n').$$

今考究直接积 $\mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_n$. 令 $a_i \to a_i'$ 是 $\mathfrak{G}_i$ 到 $\mathfrak{G}_i'$ 上的一个同构，今将証明：映照

(24) $$(a_1, a_2, \cdots, a_n) \to a_1'a_2'\cdots a_n'$$

是 $\mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_n$ 到 $\mathfrak{G}$ 上的一个同构. 这因为，首先由(23)得

$$\begin{aligned}(a_1,a_2,\cdots,a_n)(b_1,b_2,\cdots,b_n) &= (a_1b_1, a_2b_2, \cdots, a_nb_n)\\ &\to (a_1b_1)'(a_2b_2)'\cdots(a_nb_n)'\\ &= (a_1'b_1')(a_2'b_2')\cdots(a_n'b_n')\end{aligned}$$

$$= (a_1'a_2'\cdots a_n')(b_1'b_2'\cdots b_n'),$$

故映照(24)是一个同态. 因为

$$(a_1, a_2, \cdots, a_n)m = (a_1m, a_2m, \cdots, a_nm)$$
$$\rightarrow (a_1'm)(a_2'm)\cdots(a_n'm)$$
$$= (a_1'a_2'\cdots a_n')m,$$

故这映照是一个 M-映照. 因为 $\mathfrak{G}$ 的元素的形状是 $a_1'a_2'\cdots a_n'$, 这里 $a_i' \in \mathfrak{G}_i'$, 故这个映照是 $\mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_n$ 到 $\mathfrak{G}$ 上的 M-同态. 最后,考究同态核. 令 $a_1'a_2'\cdots a_n' = 1$, 则

$$(a_i')^{-1} = a_1'a_2'\cdots a_{i-1}'a_{i+1}'\cdots a_n'.$$

由(22)知, $a_i' = 1$. 于是,每个 $a_i = 1$. 故知同态核是恆等元素. 所以这映照是同构,而定理就完全証明了.

由于这个結果,所以,如果 $\mathfrak{G}_1, \mathfrak{G}_2, \cdots, \mathfrak{G}_n$ 是 M-羣 $\mathfrak{G}$ 的不变 M-子羣,适合

(25) $$\mathfrak{G} = \mathfrak{G}_1\mathfrak{G}_2\cdots\mathfrak{G}_n, \mathfrak{G}_i \cap (\mathfrak{G}_1\cdots\mathfrak{G}_{i-1}\mathfrak{G}_{i+1}\cdots\mathfrak{G}_n) = 1,$$

则説: M-羣 $\mathfrak{G}$ 是不变 M-子羣 $\mathfrak{G}_1, \mathfrak{G}_2, \cdots, \mathfrak{G}_n$ 的直接积. 严格地説,当然只能承認 $\mathfrak{G}$ 与直接积 $\mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_n$ 是同构的. 但为簡单起見,我們不強調这种区别,而逕写做 $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_n$.

作为定理 5 的判别准則的説明,我們証明下面的定理.

定理 6. 如果 $\mathfrak{G}$ 是 $n = p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ 階有限循环羣,这里 p_i 是素数,并且 $i \neq j$ 时, $p_i \neq p_j$, 則 $\mathfrak{G}$ 是 $p_i^{e_i}(i = 1, 2, \cdots, s)$ 階的循环羣的直接積.

証 令 $\mathfrak{G}_i$ 是 $p_i^{e_i}$ 阶子羣, 并令 $\mathfrak{G}' = \mathfrak{G}_1\mathfrak{G}_2\cdots\mathfrak{G}_s$. 因为 $\mathfrak{G}' \supseteq \mathfrak{G}_i$, 故这个子羣的阶数 n' 可以 $p_i^{e_i}$ 除尽. 于是, n' 可以 $n = p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ 除尽. 故 $n' = n$, 而 $\mathfrak{G}' = \mathfrak{G}$. 次令 $\mathfrak{H}_i$ 是 $\mathfrak{G}$ 的 $n_i = n/p_i^{e_i}$ 阶子羣. 令 $\mathfrak{Z}_i = \mathfrak{H}_i \cap \mathfrak{G}_i$, 則 $\mathfrak{Z}_i$ 是 $\mathfrak{G}$ 的一个子羣, 它的阶数可除尽 n_i 及 $p_i^{e_i}$. 因为 $(n_i, p_i^{e_i}) = 1$, 故知 $\mathfrak{Z}_i = 1$, 亦即 $\mathfrak{H}_i \cap \mathfrak{G}_i = 1$. 因为 $\mathfrak{H}_i$ 的阶数可以 $p_j^{e_j}(j \neq i)$ 除尽, 故 $\mathfrak{H}_i \supseteq \mathfrak{G}_j$. 于是,

$$\mathfrak{H}_i \supseteq \mathfrak{G}_1\cdots\mathfrak{G}_{i-1}\mathfrak{G}_{i+1}\cdots\mathfrak{G}_s.$$

故

$$\mathfrak{G}_1\cdots\mathfrak{G}_{i-1}\mathfrak{G}_{i+1}\cdots\mathfrak{G}_s\cap\mathfrak{G}_i=1\quad(i=1,2,\cdots,s),$$
因而适合定理 5 的各个条件.

定理 5 的条件(21)及(22)须涉及子羣 $\mathfrak{G}_i$ 間的关系，下面定理給出关于元素的条件，用在驗証上常较容易.

定理 7. 如果 $\mathfrak{G}$ 包含M-子羣 $\mathfrak{G}_i(i=1,2,\cdots,n)$，使(1)$i\neq j$时，对于任一个 $a_i\in\mathfrak{G}_i$ 及任一个 $a_j\in\mathfrak{G}_j$ 有 $a_ia_j=a_ja_i$，并且(2)$\mathfrak{G}$ 的每个元素必有而且只有一种方法寫成積 $a_1a_2\cdots a_n$，这里 $a_i\in\mathfrak{G}_i$，則

$$\mathfrak{G}=\mathfrak{G}_1\times\mathfrak{G}_2\times\cdots\times\mathfrak{G}_n.$$

証 首先要指出的是：每个 $\mathfrak{G}_i$ 是 $\mathfrak{G}$ 的不变子羣. 这因为，如果 $g_i\in\mathfrak{G}_i$，并且 $a=a_1a_2\cdots a_n, a_j\in\mathfrak{G}_j$，則由(1)知：

$$a^{-1}g_ia=a_n^{-1}\cdots a_2^{-1}a_1^{-1}g_ia_1a_2\cdots a_n=a_i^{-1}g_ia_i\in\mathfrak{G}_i.$$

但由(2)知，a 可表示 $\mathfrak{G}$ 的任一个元素，故 $\mathfrak{G}_i$ 是 $\mathfrak{G}$ 的不变子羣. 再由(2)知，$\mathfrak{G}=\mathfrak{G}_1\mathfrak{G}_2\cdots\mathfrak{G}_n$. 故 $\mathfrak{G}_1\cdots\mathfrak{G}_{i-1}\mathfrak{G}_{i+1}\cdots\mathfrak{G}_n$ 的任一个元素的形狀为 $a_1a_2\cdots a_{i-1}a_{i+1}\cdots a_n, a_j\in\mathfrak{G}_j$. 如果这个元素属于$\mathfrak{G}_i$，則有

$$a_i=a_1a_2\cdots a_{i-1}a_{i+1}\cdots a_n,\ a_j\in\mathfrak{G}_j.$$

故

$$1\cdots1a_i1\cdots1=a_1a_2\cdots a_{i-1}1a_{i+1}\cdots a_n.$$

因为每个元素只能有一种方法写成积 $a_1a_2\cdots a_n(a_j\in\mathfrak{G}_j)$，故$a_i=1$. 于是，$\mathfrak{G}_i\cap\mathfrak{G}_1\cdots\mathfrak{G}_{i-1}\mathfrak{G}_{i+1}\cdots\mathfrak{G}_n=1$. 故由定理 5 知这个定理成立.

由定理 5 的証明还看到：从条件(21)及(22)也可以推出这定理里的(1)及(2)两个条件.

下面关于子羣的直接积的重要結果至此不难导出：

A. 如果 $\mathfrak{G}=\mathfrak{G}_1\times\mathfrak{G}_2\times\cdots\times\mathfrak{G}_n$，則 $\mathfrak{G}=\mathfrak{H}_1\times\mathfrak{H}_2\times\cdots\times\mathfrak{H}_r$，这里 $\mathfrak{H}_1=\mathfrak{G}_1\mathfrak{G}_2\cdots\mathfrak{G}_{n_1}$，$\mathfrak{H}_2=\mathfrak{G}_{n_1+1}\mathfrak{G}_{n_1+2}\cdots\mathfrak{G}_{n_2}$，$\cdots,\mathfrak{H}_r=\mathfrak{G}_{n_{r-1}+1}\mathfrak{G}_{n_{r-1}+2}\cdots\mathfrak{G}_{n_r}$.

还有

$$\mathfrak{H}_1=\mathfrak{G}_1\times\mathfrak{G}_2\times\cdots\times\mathfrak{G}_{n_1},$$
$$\mathfrak{H}_2=\mathfrak{G}_{n_1+1}\times\mathfrak{G}_{n_1+2}\times\cdots\times\mathfrak{G}_{n_2},$$

(26)

$$\cdots\cdots\cdots$$

$$\mathfrak{H}_r = \mathfrak{G}_{n_{r-1}+1} \times \mathfrak{G}_{n_{r-1}+2} \times \cdots \times \mathfrak{G}_{n_r}.$$

B. 如果 $\mathfrak{G} = \mathfrak{H}_1 \times \mathfrak{H}_2 \times \cdots \times \mathfrak{H}_r$，并且(26)成立，則 $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_n$.

証明都从略．我們还有下面的結果：

C. 如果 $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2$，則 $\mathfrak{G}_2 \cong \mathfrak{G}/\mathfrak{G}_1$.

这因为，$\mathfrak{G}_1$ 是 $\mathfrak{G}$ 的不变子羣，故

$$\mathfrak{G}/\mathfrak{G}_1 = \mathfrak{G}_1\mathfrak{G}_2/\mathfrak{G}_1 \cong \mathfrak{G}_2/(\mathfrak{G}_1 \cap \mathfrak{G}_2) = \mathfrak{G}_2/1 \cong \mathfrak{G}_2,$$

所以这結果可由第二同构定理直接得出．

习　题　57

1. 从直接証明下面的結果来証明定理 6：如果 b 是 $n = p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ 阶的一个元素，則 $b = b_1b_2\cdots b_s$，这里 b_i 的阶数为 $p_i^{e_i}$.

2. 如果 $\mathfrak{G}$ 是 $n = st$ 阶循环羣，这里 $(s,t) = 1$．求証：$\mathfrak{G} = \mathfrak{H} \times \mathfrak{K}$，这里 $\mathfrak{H}$ 的阶数是 s，而 $\mathfrak{K}$ 的阶数是 t.

3. 如果 $\mathfrak{G}$ 是 $n = p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ 阶有限交換羣，这里 p_i 是不同的素数．求証：$\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_s$，这里 $\mathfrak{G}_i$ 是一个子羣，它的所有元素的阶数是 p_i 的冪.

11. 射影　令 $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_n$，这里 $\mathfrak{G}_i$ 是子羣；并令 $\eta_i (i = 1, 2, \cdots, n)$ 是 $\mathfrak{G}_i$ 到另一个 M-羣 $\bar{\mathfrak{G}}$ 内的一个同态．我們更假定，如果 $x_i \in \mathfrak{G}_i$，$x_j \in \mathfrak{G}_j$ 而且 $i \neq j$ 时，則

$$(x_i\eta_i)(x_j\eta_j) = (x_j\eta_j)(x_i\eta_i).$$

$\mathfrak{G}$ 的任一个元素 x 可写成 $x_1x_2\cdots x_n, x_i \in \mathfrak{G}_i$，故我們可以用下面式子定义从 $\mathfrak{G}$ 到 $\bar{\mathfrak{G}}$ 内的一个映照 η

(27)
$$(x_1x_2\cdots x_n)\eta = (x_1\eta_1)(x_2\eta_2)\cdots(x_n\eta_n).$$

可直接地驗証：η 是 $\mathfrak{G}$ 到 $\bar{\mathfrak{G}}$ 内的一个 M-同态.

如果 $\bar{\mathfrak{G}}$ 也是一个直接积，則这样拼合 $\mathfrak{G}_i$ 的 M-同态的方法是非常重要的．譬如，令 $\bar{\mathfrak{G}} = \bar{\mathfrak{G}}_1 \times \bar{\mathfrak{G}}_2 \times \cdots \times \bar{\mathfrak{G}}_n$，并令 η_i 是 $\mathfrak{G}_i$ 到 $\bar{\mathfrak{G}}_i$ 内的一个同态，則 $x_i\eta_i \in \bar{\mathfrak{G}}_i$，$x_j\eta_j \in \bar{\mathfrak{G}}_j$．于是，如果 $i \neq j$，則 $(x_i\eta_i)(x_j\eta_j) = (x_j\eta_j)(x_i\eta_i)$．故知 (27) 所給出的映照是 $\mathfrak{G}$ 到 $\bar{\mathfrak{G}}$ 内的一个 M-同态.

我們首先应用这个説明来定义某些自同态，而这些自同态是

与 $\mathfrak{G}$ 的直接分解为 $\mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_n$ 相伴的．設定义 ε_i 为 $\mathfrak{G}$ 的自同态，它是拼合下列各自同态而成：

$$x_1 \to 1, \cdots, x_{i-1} \to 1, x_i \to x_i, x_{i+1} \to 1, \cdots, x_n \to 1.$$

則由(27)得

(28) $$x\varepsilon_i = (x_1x_2\cdots x_n)\varepsilon_i = x_i.$$

如果 x_i 是 $\mathfrak{G}_i$ 的任一个元素，則 x_i 分解为 $\mathfrak{G}_j$ 的元素的积是

$$x_i = 1\cdots 1x_i1\cdots 1.$$

故由(28)显然有 $x_i\varepsilon_i = x_i$ 及 $x_i\varepsilon_j = 1\ (i \neq j)$． 如果 x 是 $\mathfrak{G}$ 的任一个元素，則 $x\varepsilon_i = x_i \in \mathfrak{G}_i$． 故 $(x\varepsilon_i)\varepsilon_i = x\varepsilon_i$，并且 $(x\varepsilon_i)\varepsilon_j = 1$．所以，如果以 0 表自同态 $x \to 1$，則得

(29) $$\varepsilon_i^2 = \varepsilon_i,\ \varepsilon_i\varepsilon_j = 0\ \ (i \neq j).$$

其次，我們說映照 ε_i 是正規的，就是說，它們可与 $\mathfrak{G}$ 的所有內自同构交换．这因为，如果 $x = x_1x_2\cdots x_n$, $x_i \in \mathfrak{G}_i$，而 a 是 $\mathfrak{G}$ 的任意元素，則

$$a^{-1}xa = (a^{-1}x_1a)(a^{-1}x_2a)\cdots(a^{-1}x_na),$$

并且 $a^{-1}x_ia \in \mathfrak{G}_i$．故

$$(a^{-1}xa)\varepsilon_i = a^{-1}x_ia = a^{-1}(x\varepsilon_i)a,$$

这証明了 ε_i 与由 a 决定的內自同构 C_a 可交换． 如果一个 M-自同态 ε 是正規变换，并且也是同勢变换（即 $\varepsilon^2 = \varepsilon$），則 ε 叫做射影．如果两个射影 $\varepsilon, \varepsilon'$ 有 $\varepsilon\varepsilon' = 0 = \varepsilon'\varepsilon$ 关系时，則叫做正交射影．应用这些名詞，我們可說，由分解 $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_n$ 决定的 ε_i 是正交射影．

还有連絡 ε_i 的另一个重要关系，它含有羣里映照的另一种重要合成．如果 η_1 及 η_2 是羣 $\mathfrak{G}$ 到它自身內的两个映照，我們定义和 $\eta_1 + \eta_2$ 为

(30) $$x(\eta_1 + \eta_2) = (x\eta_1)(x\eta_2).$$

这种合成在交换羣的自同态情形下前此已討論过（第二章，§12）．我們知道，和再添了积可使交换羣的自同态集合变成一个环．但在非交换情形，两个自同态的和不一定是一个自同态．

由(30)知，关于 $\mathfrak{G}$ 到它自身內的任意映照的和合成是可結合

的，但不一定可交换．因为

$$x(\eta+0)=(x\eta)(x0)=(x\eta)1=(x\eta),$$
$$x(0+\eta)=(x0)(x\eta)=1(x\eta)=(x\eta).$$

故自同态 0 ($x\to 1$) 在加法上起恆等元素的作用．如果我們定义 $-\eta$ 为 $x(-\eta)=(x\eta)^{-1}$，則

$$x(-\eta+\eta)=(x\eta)^{-1}(x\eta)=1,$$
$$x(\eta+(-\eta))=(x\eta)(x\eta)^{-1}=1.$$

故 $-\eta+\eta=0=\eta+(-\eta)$．这証明：$\mathfrak{G}$ 里映照的集合与加法合成是一个羣．

映照的乘法关于加法适合右分配律

(31) $$\rho(\eta_1+\eta_2)=\rho\eta_1+\rho\eta_2;$$

这因为

$$x\rho(\eta_1+\eta_2)=((x\rho)\eta_1)((x\rho)\eta_2),$$
$$x(\rho\eta_1+\rho\eta_2)=(x(\rho\eta_1))(x(\rho\eta_2))=((x\rho)\eta_1)((x\rho)\eta_2).$$

但左分配律一般不能成立．如果 ρ 是一个自同态，因为

$$x((\eta_1+\eta_2)\rho)=((x\eta_1)(x\eta_2))\rho=((x\eta_1)\rho)((x\eta_2)\rho)$$
$$=(x(\eta_1\rho))(x(\eta_2\rho))=x(\eta_1\rho+\eta_2\rho),$$

此时左分配律仍能成立．

今回到由直接分解 $\mathfrak{G}=\mathfrak{G}_1\times\mathfrak{G}_2\times\cdots\times\mathfrak{G}_n$ 所决定的射影 ε_i 的考究．如果 x 是 $\mathfrak{G}$ 的任一个元素，則 $x=x_1x_2\cdots x_n$，这里 $x_i\in\mathfrak{G}_i$．于是，

$$x=(x\varepsilon_1)(x\varepsilon_2)\cdots(x\varepsilon_n),$$

故由加法及 1 的定义得

(32) $$\varepsilon_1+\varepsilon_2+\cdots+\varepsilon_n=1.$$

(29)及(32)两个性质是由直接分解所决定的射影的特性．故設 $\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n$ 是适合(29)及(32)的正規 M-自同态，則 $\mathfrak{G}_i=\mathfrak{G}\varepsilon_i$ 是一个 M-子羣，并且因为

$$a^{-1}(x\varepsilon_i)a=(a^{-1}xa)\varepsilon_i\in\mathfrak{G}_i,$$

故 $\mathfrak{G}_i$ 是不变子羣．因为

$$x=x1=x(\varepsilon_1+\varepsilon_2+\cdots+\varepsilon_n)=(x\varepsilon_1)(x\varepsilon_2)\cdots(x\varepsilon_n),$$

故 $\mathfrak{G}=\mathfrak{G}_1\mathfrak{G}_2\cdots\mathfrak{G}_n$．其次，因为 $\mathfrak{G}_i=\mathfrak{G}\varepsilon_i$，故 ε_i 是 $\mathfrak{G}_i$ 里恆等映

照. 并且在 $j \neq i$ 时, ε_i 把 $\mathfrak{G}_j$ 映照到 1. 所以, 如果 $x \in \mathfrak{G}_i \cap \mathfrak{G}_1\mathfrak{G}_2\cdots\mathfrak{G}_{i-1}\mathfrak{G}_{i+1}\cdots\mathfrak{G}_n$, 则有 $x\varepsilon_i = x$, 又有 $x\varepsilon_i = 1$, 故

$$\mathfrak{G}_i \cap \mathfrak{G}_1\mathfrak{G}_2\cdots\mathfrak{G}_{i-1}\mathfrak{G}_{i+1}\cdots\mathfrak{G}_n = 1.$$

于是, $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_n$. 因为 $x = (x\varepsilon_1)(x\varepsilon_2)\cdots(x\varepsilon_n)$, 而 $x\varepsilon_i \in \mathfrak{G}_i$, 故由这个分解所决定的射影是給定的映照 ε_i. 我們的討論就到此为止.

习　题 58

1. 如果 η 是一个正規自同态, 求証: η 的形状是 $a\eta = c(a,\eta)a$, 这里 $c(a,\eta)$ 是与 $\mathfrak{G}\eta$ 的各元素可交换的一个元素, 并且 $c(ab,\eta) = c(a,\eta)[ac(b,\eta)a^{-1}]$.

2. 如果心 $\mathfrak{C} = 1$, 或者换位子羣 $\mathfrak{G}^{(1)} = \mathfrak{G}$ (参看习題 51 第 3 題定义), 求証: 恆等映照是 $\mathfrak{G}$ 的唯一正規自同构.

3. 令 $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$ 是一个直接分解的射影. 如果 $i_1, i_2, \cdots, i_r$ 不相同, 求証: $\varepsilon_{i_1} + \varepsilon_{i_2} + \cdots + \varepsilon_{i_r}$ 是一个自同态, 并求証: $\varepsilon_i + \varepsilon_j = \varepsilon_j + \varepsilon_i$.

12. 分解为不可分解羣 如果一个 M-羣 $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2$, 这里各个 $\mathfrak{G}_i$ 是眞子羣, 则說 $\mathfrak{G}$ 是可分解的. 于是, $\mathfrak{G}_i \neq 1$. 故射影 $\varepsilon_i(i = 1,2) \neq 1$, 并且也 $\neq 0$. 所以, 如果 $\mathfrak{G}$ 是可分解的, 则有 $\mathfrak{G}$ 的射影存在, 它們 $\neq 1, 0$. 反过来, 它也是 $\mathfrak{G}$ 成为可分解的充分条件. 这因为, 令 ε_1 是一个射影, $\neq 1, 0$. 命 $\mathfrak{G}_1 = \mathfrak{G}\varepsilon_1$, 并令 $\mathfrak{G}_2$ 是自同态 ε_1 的核, 则 $\mathfrak{G}_1$ 及 $\mathfrak{G}_2$ 都是 M-子羣; 且因为 ε_1 的正規性, 这两个子羣都是不变子羣. 如果 x 是 $\mathfrak{G}$ 的任一个元素, 因为

$$((x\varepsilon_1)^{-1}x)\varepsilon_1 = ((x\varepsilon_1)^{-1}\varepsilon_1)(x\varepsilon_1) = (x\varepsilon_1^2)^{-1}(x\varepsilon_1) = 1,$$

故 $z = x(-\varepsilon_1 + 1) = (x\varepsilon_1)^{-1}x \in \mathfrak{G}_2$. 于是, $x = (x\varepsilon_1)z \in \mathfrak{G}_1\mathfrak{G}_2$. 其次, 如果 x_1 是 $\mathfrak{G}_1$ 的任一个元素, 则 $\mathfrak{G}$ 里有一个 x 使 $x_1 = x\varepsilon_1$. 于是, $x_1 = x\varepsilon_1 = x\varepsilon_1^2 = x_1\varepsilon_1$. 故 $\mathfrak{G}_1 \cap \mathfrak{G}_2 = 1$. 因此, $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2$. 因为 $\varepsilon_1 \neq 1, 0$, 故 $\mathfrak{G}_1 \neq \mathfrak{G}$, $\mathfrak{G}_2 \neq \mathfrak{G}$, 而 $\mathfrak{G}$ 是可分解的. 因此得下面的定理.

定理 8. 一个 M-羣 $\mathfrak{G}$ 是可分解的充要条件是存在有 $\mathfrak{G}$ 的射影, 它們 $\neq 1$, $\neq 0$.

其次, 我們要証明, 任一个羣 $\mathfrak{G} \neq 1$ 如果适合不变 M-子羣的降鏈条件, 则 $\mathfrak{G}$ 可分解为不可分解 M-羣的直接积. 我們所作的假

定是:

I′. 如果 $\mathfrak{G}_1 \supseteq \mathfrak{G}_2 \supseteq \mathfrak{G}_3 \supseteq \cdots$ 是 $\mathfrak{G}$ 的不变 M-子羣的递降序列，则有一个整数 N 存在，使 $\mathfrak{G}_N = \mathfrak{G}_{N+1} = \cdots$.

我們应用这个条件先証：$\mathfrak{G}$ 有一个不可分解的直接因子. 这因为，$\mathfrak{G}$ 或是不可分解的，或是 $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2$，而 $\mathfrak{G}_1 \neq \mathfrak{G}, \neq 1$. 如果 $\mathfrak{G}_1$ 是不可分解的，它便是所求的因子了. 否則，$\mathfrak{G}_1 = \mathfrak{G}_{11} \times \mathfrak{G}_{12}$，这里 $\mathfrak{G}_{11} \neq \mathfrak{G}_1, \neq 1$. 于是，$\mathfrak{G} \supset \mathfrak{G}_1 \supset \mathfrak{G}_{11}$，而 $\mathfrak{G}_{11}$ 或是不可分解的，或是 $\mathfrak{G}_{11} = \mathfrak{G}_{111} \times \mathfrak{G}_{112}$，而 $\mathfrak{G}_{111} \neq \mathfrak{G}_{11}, \neq 1$. 此时就得出較长的鏈 $\mathfrak{G} \supset \mathfrak{G}_1 \supset \mathfrak{G}_{11} \supset \mathfrak{G}_{111}$. 依这样得来所有的羣都是 $\mathfrak{G}$ 的不变 M-子羣. 于是，I′ 保証这种分解只能經过有限步驟即达到一个不可分解的直接因子.

今令 $\mathfrak{G}_1$ 表示 $\mathfrak{G}$ 的一个不可分解的直接因子，令 $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_1'$. 如果 $\mathfrak{G}_1' \neq 1$，则可分解为 $\mathfrak{G}_1' = \mathfrak{G}_2 \times \mathfrak{G}_2'$，这里 $\mathfrak{G}_2$ 是不可分解的. 于是，$\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2 \times \mathfrak{G}_2'$，而 $\mathfrak{G}_2'$ 是 $\mathfrak{G}$ 的不变子羣. 至此，$\mathfrak{G}_2'$ 或是 $=1$，或是 $\mathfrak{G}_2' = \mathfrak{G}_3 \times \mathfrak{G}_3'$，这里 $\mathfrak{G}_3$ 是不可分解的，而 $\mathfrak{G}_3'$ 是 $\mathfrak{G}$ 的不变子羣. 这个方法导出不变 M-子羣的眞降鏈 $\mathfrak{G} \supset \mathfrak{G}_1' \supset \mathfrak{G}_2' \supset \mathfrak{G}_3' \supset \cdots$. 再由 I′ 知，有整数 n 存在使 $\mathfrak{G}_n' = 1$. 于是，$\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_n$，这里 $\mathfrak{G}_i$ 都是不可分解的. 这証明了

定理 9. 如果任一个 M-羣 $\neq 1$，并且适合不变 M-子羣的降鏈条件，则可寫成有限个不可分解羣（$\neq 1$）的直接積.

13. 克魯尔-叔密特定理 本节将证关于分解一个 M-羣为不可分解羣的直接积的唯一性定理. 要建立这个結果，除降鏈条件 I′ 外，还需要下面的升鏈条件：

II′. 如果 $\mathfrak{G}_1 \subseteq \mathfrak{G}_2 \subseteq \mathfrak{G}_3 \subseteq \cdots$ 是不变 M-子羣的一个递升序列，则有整数 N 存在，使 $\mathfrak{G}_N = \mathfrak{G}_{N+1} = \cdots$.

今来考究鏈条件的一些重要結果. 我們先証下面的定理.

定理 10. 令 $\mathfrak{G}$ 是一个 M-羣，适合不变 M-子羣的升鏈及降鏈条件. 如果 η 是一个正規 M-自同态，并且 (1) η 是 1—1 映照，或 (2) 使 $\mathfrak{G}\eta = \mathfrak{G}$，则 η 是一个自同構.

証　假定 η 是 1—1 映照. 如果对于某一个 $r = 1, 2, \cdots$ 有

$\mathfrak{G}\eta^{r-1} = \mathfrak{G}\eta^r$，则对于 $\mathfrak{G}\eta^{r-2}$ 里任一个 y，必有一个元素 x 存在，使 $y\eta = x\eta^r = (x\eta^{r-1})\eta$．于是，$y = x\eta^{r-1} \in \mathfrak{G}\eta^{r-1}$．但 $\mathfrak{G}\eta^{r-2} \supseteq \mathfrak{G}\eta^{r-1}$，故 $\mathfrak{G}\eta^{r-2} = \mathfrak{G}\eta^{r-1}$．重复这样論証継續下去，最后得 $\mathfrak{G} = \mathfrak{G}\eta$．故知，如果 $\mathfrak{G} \supset \mathfrak{G}\eta$，则 $\mathfrak{G} \supset \mathfrak{G}\eta \supset \mathfrak{G}\eta^2 \supset \cdots$ 是一个无限眞降鏈．但因 η 是一个正規 M-自同态，故这个鏈的所有項都是不变 M-子羣．这与条件 I′ 矛盾．于是，如果 η 是 1—1 映照，则 $\mathfrak{G} = \mathfrak{G}\eta$，从而 η 是一个自同构．次設 $\mathfrak{G} = \mathfrak{G}\eta$．令 $\mathfrak{Z}_k$ 表示自同态 $\eta^k (k = 0,1,2,\cdots)$ 的核，而 $\eta^0 \equiv 1$．因为采取 $\eta^0 = 1$，故 $\mathfrak{Z}_0 = 1$．显然，$\mathfrak{Z}_{k-1} \subseteq \mathfrak{Z}_k$．今設 $\mathfrak{Z}_{r-1} = \mathfrak{Z}_r$，并令 $z \in \mathfrak{Z}_{r-1}$，则可写 $z = y\eta$．于是，

$$1 = z\eta^{r-1} = (y\eta)\eta^{r-1} = y\eta^r.$$

因为 $\mathfrak{Z}_{r-1} = \mathfrak{Z}_r$，故 $y\eta^{r-1} = 1$，并且 η^{r-2} 把 $z = y\eta$ 映到 1．因此，$z \in \mathfrak{Z}_{r-2}$．这証明 $\mathfrak{Z}_{r-2} = \mathfrak{Z}_{r-1}$．这样継續下去，可知所有 $\mathfrak{Z}_k = 1$．于是，或者 $\mathfrak{Z}_1 = 1$，或者

$$1 = \mathfrak{Z}_0 \subset \mathfrak{Z}_1 \subset \mathfrak{Z}_2 \subset \cdots$$

是不变 M-子羣的一个无限眞升鏈．但后者与 II′ 矛盾；故知，如果 $\mathfrak{G}\eta = \mathfrak{G}$，则 $\mathfrak{Z}_1 = 1$，并且 η 是 1—1 映照．

如果 η 是一个羣的任一个自同态，则对于某个整数 s 能使 $z\eta^s = 1$ 的元素 z 的全体叫做 η 的**根集**．故根集 $\mathfrak{R}$ 是同态 η^i 的核 $\mathfrak{Z}_i$ 的集合論上的和．我們应用这个概念来叙述下面的定理，它是証明唯一性定理的关鍵．

定理 11（費廷(Fitting)引理）．令 $\mathfrak{G}$ 是一个 M-羣，适合不变 M-子羣的兩个鏈条件，η 是 $\mathfrak{G}$ 的一个正規 M-自同态，则 $\mathfrak{G} = \mathfrak{R} \times \mathfrak{H}$，这里 $\mathfrak{R}$ 是 η 的根集，而 $\mathfrak{H}$ 适合 $\mathfrak{H}\eta = \mathfrak{H}$ 的条件．

証　有不变 M-子羣的降鏈 $\mathfrak{G} \supseteq \mathfrak{G}\eta \supseteq \mathfrak{G}\eta^2 \supseteq \cdots$，故有一个整数 r 存在使 $\mathfrak{G}\eta^r = \mathfrak{G}\eta^{r+1}$．于是，$\mathfrak{G}\eta^r = \mathfrak{G}\eta^{r+1} = \mathfrak{G}\eta^{r+2} = \cdots$．令 $\mathfrak{H}$ 表示这个不变 M-子羣．次考究升鏈 $\mathfrak{Z}_0 \subseteq \mathfrak{Z}_1 \subseteq \mathfrak{Z}_2 \subseteq \cdots$，这里 $\mathfrak{Z}_i$ 是 η^i 的核，则有一个整数 s 存在，使 $\mathfrak{Z}_s = \mathfrak{Z}_{s+1}$．于是，有 $\mathfrak{Z}_{s+1} = \mathfrak{Z}_{s+2} = \cdots$．故 $\mathfrak{Z}_s$ 是 η 的根集 $\mathfrak{R}$．令 t 是 r，s 中較大的整数．如果 x 是 $\mathfrak{G}$ 里任一个元素，则有一个 y 使 $x\eta^t = y\eta^{2t}$．于是，$x = [x(y\eta^t)^{-1}](y\eta^t)$，并且 $[x(y\eta^t)^{-1}]\eta^t = (x\eta^t)(y\eta^{2t})^{-1} = 1$．所以，

如果令 $z = x(y\eta^t)^{-1}$，则 $z\eta^t = 1$，而 $z \in \mathfrak{R}$. 因为 $y\eta^t \in \mathfrak{H}$，故得$\mathfrak{G}$的分解 $\mathfrak{G} = \mathfrak{R}\mathfrak{H}$. 今令 $w \in \mathfrak{R} \cap \mathfrak{H}$，则 $w = u\eta^t$，并且 $1 = w\eta^t = u\eta^{2t}$. 于是，$u \in \mathfrak{R}$，并且 $u\eta^t = 1$. 故$w = 1$. 因此，$\mathfrak{G} = \mathfrak{R} \times \mathfrak{H}$.

因为 $\mathfrak{R} = \mathfrak{Z}_t$，故对于每个 $z \in \mathfrak{R}$ 显然有 $z\eta^t = 1$. 这意味着 η 是 $\mathfrak{R}$ 里一个无势自同态. 如果 $\mathfrak{G}$ 是不可分解的，则 $\mathfrak{G} = \mathfrak{R}$，或者 $\mathfrak{G} = \mathfrak{H}$. 如果 $\mathfrak{G} = \mathfrak{R}$，则 η 是无势的；如果 $\mathfrak{G} = \mathfrak{H}$，则 η 是1—1映照，并由定理10知，η 是一个自同构. 这証明了

系 1 設 $\mathfrak{G}$ 是一个不可分解的 M–羣，适合不变 M–子羣的兩个鏈条件，则 $\mathfrak{G}$ 的任一个正規 M–自同态是无势的，或是一个自同構.

由这个系使我們能証得关于一个不可分解羣的正規无势自同态的极有趣的封閉性質，即

系 2 令 $\mathfrak{G}$ 是一个不可分解的 M–羣，适合不变 M–子羣的兩个鏈条件，并令 η_1 及 η_2 是正規无势 M–自同态. 如果 $\eta_1 + \eta_2$ 是一个自同态，则 $\eta_1 + \eta_2$ 是无势 M–自同态.

証 根据系 1，如果 $\eta = \eta_1 + \eta_2$ 不是无势的，则必是一个自同构. 令 η^{-1} 是它的逆变换，显然这个映照是一个正規 M–自同态，且 $\eta_1\eta^{-1} + \eta_2\eta^{-1} = 1$，或 $\lambda_1 + \lambda_2 = 1$，这里 $\lambda_i = \eta_i\eta^{-1}$. 因为 η_i 不是一个自同构，它的核 $\neq 1$，故对于 λ_i 也成立. 于是，λ_i 是无势的. 但因 $\lambda_1 = \lambda_1(\lambda_1 + \lambda_2) = \lambda_1^2 + \lambda_1\lambda_2$，又 $\lambda_1 = (\lambda_1 + \lambda_2)\lambda_1 = \lambda_1^2 + \lambda_2\lambda_1$，所以 $\lambda_1\lambda_2 = \lambda_2\lambda_1$. 于是，对于任一个正整数$m$有

$$(\lambda_1 + \lambda_2)^m = \lambda_1^m + \binom{m}{1}\lambda_1^{m-1}\lambda_2 + \binom{m}{2}\lambda_1^{m-2}\lambda_2^2 + \cdots + \lambda_2^m. \tag{33}$$

今令 $\lambda_1^r = 0$，$\lambda_2^s = 0$，并于上面恆等式里取 $m = r + s - 1$，则得 $1 = 0$ 的矛盾. 故 $\eta_1 + \eta_2$ 是无势的.

习 题 59

1. 令 $\mathfrak{G}$ 适合 I′ 及 II′，并令 η 是一个正規自同态. 令 r 是第一个整数能使 $\mathfrak{G}\eta^r = \mathfrak{G}\eta^{r+1}$，并令 s 是第一个整数能使 $\mathfrak{Z}_s = \mathfrak{Z}_{s+1}$，这里 $\mathfrak{Z}_i$ 是 η^i 的核. 求証：$r = s$.

今来証主要的定理：

克鲁尔-叔密特定理 令 $\mathfrak{G}$ 是一个 M-群，适合不变 M-子群的两个鏈条件，并令

(34) $$\mathfrak{G}=\mathfrak{G}_1\times\mathfrak{G}_2\times\cdots\times\mathfrak{G}_s,$$

(35) $$\mathfrak{G}=\mathfrak{H}_1\times\mathfrak{H}_2\times\cdots\times\mathfrak{H}_t$$

是 $\mathfrak{G}$ 分解为不可分解群的两个直接分解，则 $s=t$，并且 $\mathfrak{H}_i$ 經适宜編列后有 $\mathfrak{H}_i\cong\mathfrak{G}_i$，并且

(36) $$\mathfrak{G}=\mathfrak{H}_1\times\cdots\times\mathfrak{H}_k\times\mathfrak{G}_{k+1}\times\cdots\times\mathfrak{G}_s$$
$$(k=1,2,\cdots,s).$$

証 假設已得到与 $\mathfrak{G}_1,\mathfrak{G}_2,\cdots,\mathfrak{G}_{r-1}$ 顺序成配对的 $\mathfrak{H}_1,\mathfrak{H}_2,\cdots,\mathfrak{H}_{r-1}$，使 $\mathfrak{G}_i\cong\mathfrak{H}_i(i=1,2,\cdots,r-1)$，并且(36)在 $k\leqslant r-1$ 时成立(开始取 $r=1$，显然成立)。今考究中間分解

(37) $$\mathfrak{G}=\mathfrak{H}_1\times\mathfrak{H}_2\times\cdots\times\mathfrak{H}_{r-1}\times\mathfrak{G}_r\times\cdots\times\mathfrak{G}_s.$$

令 $\lambda_1,\lambda_2,\cdots,\lambda_s$ 是由这个分解所决定的射影，并令 $\eta_1,\eta_2,\cdots,\eta_t$ 是由(35)所决定的射影。显然，$\lambda_r=\left(\sum_1^t\eta_i\right)\lambda_r=\sum_1^t\eta_j\lambda_r$。因为 $\mathfrak{G}$ 里任一个 x 都有 $x\eta_j\in\mathfrak{H}_j$；所以，如果 $j\leqslant r-1$，則由(37)得 $x\eta_j=x\eta_j\lambda_j$ 及 $x\eta_j\lambda_r=x\eta_j\lambda_j\lambda_r=1$。故 $\eta_j\lambda_r=0$，而得关系

(38) $$\lambda_r=\eta_r\lambda_r+\eta_{r+1}\lambda_r+\cdots+\eta_t\lambda_r.$$

今把它施于 $\mathfrak{G}_r$ 里。因为此时 $\lambda_r=1$，故得 $1=\sum_r^t\eta_j\lambda_r$。再則任一个部分和 $\sum\eta_{i_l}\lambda_r=(\sum\eta_{i_l})\lambda_r$ 在 $\mathfrak{G}_r$ 里导出一个正規 M-自同态。因为 $\mathfrak{G}_r$ 是不可分解的，故由系 2 知，有一个 $u(r\leqslant u\leqslant t)$ 存在使 $\eta_u\lambda_r$ 定义 $\mathfrak{G}_r$ 的一个自同构。我們可改編 $\mathfrak{H}_i(i=r,r+1,\cdots)$ 使 $\mathfrak{H}_u$ 变为 $\mathfrak{H}_r$。今来証明：$\mathfrak{G}_r\cong\mathfrak{H}_r$，并且(36)对于 $k=r$ 成立。

因为 $\eta_r\lambda_r$ 是 $\mathfrak{G}_r$ 里一个自同构，它的核是 1。故 $\mathfrak{G}_r$ 里的 z 能使 $z\eta_r=1$ 时，則 $z=1$。于是，η_r 把 $\mathfrak{G}_r$ 同构地映照到 $\mathfrak{H}_r$ 內。令 $\bar{\mathfrak{H}}_r=\mathfrak{G}_r\eta_r$，并令 $\mathfrak{U}_r$ 表示 $\mathfrak{H}_r$ 里使 $u\lambda_r=1$ 的元素 u 的集合。因为 λ_r 是 $\bar{\mathfrak{H}}_r=\mathfrak{G}_r\eta_r$ 到 $\mathfrak{G}_r$ 內的一个同构，故 $\bar{\mathfrak{H}}_r\cap\mathfrak{U}_r=1$。又若 y 是 $\mathfrak{H}_r$ 的任一个元素，則 $y\lambda_r\in\mathfrak{G}_r$，故 $\mathfrak{G}_r$ 里有一个 v 使 $y\lambda_r=v\eta_r\lambda_r$。我們可把 y 写成 $y=(y(v\eta_r)^{-1})(v\eta_r)$，并知 $y(v\eta_r)^{-1}\in\mathfrak{U}_r$，而 $v\eta_r\in\bar{\mathfrak{H}}_r$.

故 $\mathfrak{H}_r = \mathfrak{U}_r\bar{\mathfrak{H}}_r = \mathfrak{U}_r \times \bar{\mathfrak{H}}_r$. 因为 $\mathfrak{H}_r$ 是不可分解的，幷且 $\mathfrak{H}_r \neq 1$，故 $\mathfrak{H}_r = \bar{\mathfrak{H}}_r = \mathfrak{G}_r\eta_r$. 所以 η_r 是 $\mathfrak{G}_r$ 到 $\mathfrak{H}_r$ 上的一个同构，而 λ_r 是 $\mathfrak{H}_r = \mathfrak{G}_r\eta_r$ 到 $\mathfrak{G}_r$ 上的一个同构.

但 λ_r 把 $\mathfrak{H}_1 \times \cdots \times \mathfrak{H}_{r-1} \times \mathfrak{G}_{r+1} \times \cdots \times \mathfrak{G}_s$ 的各元素映到 1 上，又因为 λ_r 导出 $\mathfrak{H}_r$ 的一个同构，故

$$\mathfrak{H}_r \cap (\mathfrak{H}_1 \cdots \mathfrak{H}_{r-1}\mathfrak{G}_{r+1} \cdots \mathfrak{G}_s) = 1.$$

于是

(39) $$\mathfrak{G}' \equiv \mathfrak{H}_1 \cdots \mathfrak{H}_r\mathfrak{G}_{r+1} \cdots \mathfrak{G}_s = \mathfrak{H}_1 \times \cdots \times \mathfrak{H}_r \times \mathfrak{G}_{r+1} \times \cdots \times \mathfrak{G}_s.$$

如果 $x = x_1x_2 \cdots x_s$，这里 $i \leqslant r-1$ 时，$x_i \in \mathfrak{H}_i$，而 $j \geqslant r$ 时 $x_j \in \mathfrak{G}_j$，則映照

$$\theta: x_1x_2 \cdots x_s \to x_1 \cdots x_{r-1}(x_r\eta_r)x_{r+1} \cdots x_s$$

是 $\mathfrak{G}$ 的一个正規 M-自同态. 显然 θ 是 $\mathfrak{G}$ 到 $\mathfrak{G}'$ 上的一个同构. 故由定理 10 得 $\mathfrak{G}' = \mathfrak{G}$. 于是，(36)在 $k = r$ 时也成立. 这就完成了証明.

如果(34)及(35)成立，幷且 μ_i 是 $\mathfrak{G}_i$ 到 $\mathfrak{H}_i$ 上的一个 M-同构，則由

$$x\mu = (x_1x_2 \cdots x_s)\mu = (x_1\mu_1)(x_2\mu_2) \cdots (x_s\mu_s), (x_i \in \mathfrak{G}_i)$$

定义的映照 μ 显然是一个正規 M-自同构. 我們易知，$\mathfrak{G}_i\mu = \mathfrak{H}_i$. 故唯一性定理的第一部分也可述成下面形状:

如果(34)及(35)是适合兩个鏈条件的一个 M-羣的兩种分解成不可分解的因子，則 $s = t$，幷且把 $\mathfrak{H}_i$ 的次序适当編列后，則有一个正規自同構 μ 存在，使 $\mathfrak{G}_i\mu = \mathfrak{H}_i$.

习 題 60

在下面各題里假定不变 M-子羣的两个鏈条件都成立.

1. 如果 $\mathfrak{G}$ 的心 $=1$，或者 $\mathfrak{G} = \mathfrak{G}^{(1)}$，求証: $\mathfrak{G}$ 只有一种分解成不可分解羣的直接积.

2. 令 $\xi_1, \xi_2, \cdots, \xi_s$ 及 $\eta_1, \eta_2, \cdots, \eta_s$ 是由 $\mathfrak{G}$ 分解为不可分解羣的两种直接分解所决定的射影. 如果适当地选取 η 的次序，求証: 必有一个正規自同构 μ 存在，使 $\eta_i = \mu^{-1}\xi_i\mu (i = 1, 2, \cdots, s)$.

3. 如果羣 $\mathfrak{G}$ 的不可分解的因子是同构的，則 $\mathfrak{G}$ 叫做齐次羣. 如果射影 ε 使 $\mathfrak{G}\varepsilon$

是不可分解羣，则这 ε 叫做**原射影**. 令 ε 及 ε' 是齐次羣的原射影，求証：必有一个正規 M-自同构 μ 存在，使 $\varepsilon' = \mu^{-1}\varepsilon\mu$.

14. 无限直接积 今将考究把有限个羣的直接积的作法拓广到任意个羣去. 在处理羣的任意集合中，为方便起見，假設羣附注下标 α，是取自某集合 J 的；而且同一个羣可計算多次，亦即 $\alpha \neq \beta$ 时，我們不需要 $\mathfrak{G}_\alpha \neq \mathfrak{G}_\beta$. 因此，我們有一个集合 $J = \{\alpha\}$，子羣的集合 $\{\mathfrak{G}\}$，及 J 到 $\{\mathfrak{G}\}$ 上的单值映照 $\alpha \to \mathfrak{G}_\alpha$.

今先定义 $\mathfrak{G}_\alpha$ 的积集合 $\widetilde{\prod\limits_{\alpha \in J}} \mathfrak{G}_\alpha$. 这集合的元素是"向量" $(\cdots g_\alpha \cdots)$，它的"α-位"上的元素属于集合 $\mathfrak{G}_\alpha$. 更精确地說，$\widetilde{\Pi}$ 的元素是 J 的单值映照 $\alpha \to g_\alpha$，它使 J 里每个 α 的象 g_α 属于相伴羣 $\mathfrak{G}_\alpha$. 因此，如果 g 表示 $\widetilde{\Pi}$ 的一个元素，則可采用通常的函数記法 $g(\alpha)$ 来表示象元素 g_α.

如果 J 是正整数的集合 $\{1, 2, 3, \cdots\}$，則 $\widetilde{\Pi}$ 是序列 $(g_1, g_2, \cdots)$ 的集合，这里 $g_i = g(i) \in \mathfrak{G}_i$ $(i = 1, 2, 3, \cdots)$. 我們还須知道，如果 J 是任意的，而所有 $\mathfrak{G}_\alpha = \mathfrak{G}$，則 $\widetilde{\Pi}$ 是 J 到 $\mathfrak{G}$ 內的映照的全集. 如果沿用对于环的記法(第三章，§12)，則这个集合还可記作 $(\mathfrak{G}, J)$.

今应用 $\mathfrak{G}_\alpha$ 是羣的事实，在 $\widetilde{\Pi}$ 里引入支量的乘法. 譬如，g 及 $h \in \widetilde{\Pi}$，則 gh 用方程

$$(gh)(\alpha) = g(\alpha)h(\alpha) \tag{40}$$

来定义. 因为 $(gh)(\alpha) \in \mathfrak{G}_\alpha$，故 $gh \in \widetilde{\Pi}$. 由此可見，$\widetilde{\Pi}$ 及这种乘法构成一个羣. $\widetilde{\Pi}$ 的恆等元素 1 是：对于所有 α 能使 $1(\alpha) = 1$ 的函数；而 $g^{-1}(\alpha) = g(\alpha)^{-1}$. 如果所有 $\mathfrak{G}_\alpha$ 是 M-羣，則 $\widetilde{\Pi}$ 也可看作一个 M-羣. 为着这个目的，我們以

$$(gm)(\alpha) = g(\alpha)m \tag{41}$$

来定义 gm. 由此可見它适合基本条件(1). 这样得出的 M-羣叫做 M-羣 $\mathfrak{G}_\alpha$ 的**完全直接积**.

今令 $\mathfrak{H}$ 是 M-羣 $\widetilde{\Pi}$ 的任一个子羣，而考究 $\mathfrak{H}$ 到 $\mathfrak{G}_\alpha$ 內的映照 $h \to h(\alpha)$. 由(40)及(41)显然知道，这个映照是 $\mathfrak{H}$ 到 $\mathfrak{G}_\alpha$ 內的一个同态. 象 $\mathfrak{H}_\alpha$ 是 $\mathfrak{G}_\alpha$ 的一个 M-子羣. 如果对于所有 α，$\mathfrak{H}_\alpha = \mathfrak{G}_\alpha$，亦

即如果对于 J 里各 α，同态 $h \to h(\alpha)$ 是一个到 $\mathfrak{G}_\alpha$ 上的映照，则說 $\mathfrak{H}$ 是 $\mathfrak{G}_\alpha$ 的子直接积. 显然，$\mathfrak{H}$ 总是象羣 $\mathfrak{H}_\alpha$ 的一个子直接积.

現在要定义一种特別有趣的子直接积. 設 $\widetilde{\Pi}$ 里元素 g 对于除有限个以外的所有 α 具有性質 $g(\alpha)=1$，这样元素的全体記作 $\prod_{\alpha \in J} \mathfrak{G}_\alpha$. 如果 $\alpha \neq \alpha_1, \alpha_2, \cdots, \alpha_m$ 时，$g(\alpha)=1$，而 $\alpha \neq \beta_1, \beta_2, \cdots, \beta_n$ 时，$h(\alpha)=1$. 则在 $\alpha \neq \alpha_1, \cdots, \alpha_m$; $\beta_1, \cdots, \beta_n$ 时，$(gh)(\alpha)=1$. 故 Π 对于乘法封閉. 显然，$1 \in \Pi$，并且如果 $g \in \Pi$，则 $g^{-1} \in \Pi$. 故 Π 是 $\widetilde{\Pi}$ 的一个子羣.

对于 J 里任一个 γ，如果当 $\alpha \neq \gamma$ 时，有 $g(\alpha)=1$，这样元素 g 所成的子集合命为 $\mathfrak{G}'_\gamma$，显然 $\mathfrak{G}'_\gamma$ 是 Π 的一个子羣，并且映照 $h \to h(\gamma)$ 是 $\mathfrak{G}'_\gamma$ 到 $\mathfrak{G}_\gamma$ 上的一个同构. 由此当然推出：对于 J 里的每个 γ，映照 $h \to h(\gamma)$ 是 Π 到 $\mathfrak{G}_\gamma$ 上的一个同态. 故 Π 是 $\mathfrak{G}_\alpha$ 的一个子直接积. 这个特殊的子直接积叫做 $\mathfrak{G}_\alpha$ 的直接积. 如果 J 是一个有限集合（并且只有这种情形），则 $\Pi = \widetilde{\Pi}$.

在这有限的情形下，我們可用羣 $\mathfrak{G}'_\gamma$ 显出 Π 的特性. 譬如，我們易知，$\mathfrak{G}'_\gamma$ 是 Π 的不变 M-子羣，并且

1. $$\prod_{\alpha \in J} \mathfrak{G}_\alpha = [\cup \mathfrak{G}'_\alpha],$$

2. $$\mathfrak{G}'_\beta \cap \left[\bigcup_{\alpha \neq \beta} \mathfrak{G}'_\alpha \right] = 1.$$

这里 $[\cup \mathfrak{G}'_\alpha]$ 也象慣用的記法，表示由羣 $\mathfrak{G}'_\alpha$ 生成的子羣. 反过来，如果 $\mathfrak{G}$ 是任一个 M-羣，它含有适合 1 及 2 的不变 M-子羣 $\mathfrak{G}'_\alpha$，则 $\mathfrak{G}$ 与 $\mathfrak{G}'_\alpha$ 的直接积是同构的. 此时，我們也簡单地說，$\mathfrak{G}$ 是它的子羣的直接积，而就記作 $\mathfrak{G} = \Pi \mathfrak{G}'_\alpha$.

习　题　61

1. 令 $\mathfrak{G}$ 是一个交換羣，沒有无限阶的元素. 对于每个素数 p，令 $\mathfrak{G}_p$ 是由阶数等于 p 的冪的元素所构成的子集合. 求証：$\mathfrak{G}_p$ 是 $\mathfrak{G}$ 的一个子羣，并且 $\mathfrak{G} = \prod_p \mathfrak{G}_p$.

2. 如果前題里所考究的羣 $\mathfrak{G}$ 是一个环的加法羣，求証：$\mathfrak{G}_p$ 是理想. 所以环 $\mathfrak{G}$

是直接和$\sum\limits_{p}\oplus\mathfrak{S}_p$[1]，并且当 $p\neq q$ 时，$\mathfrak{S}_p\mathfrak{S}_q=0$。

3．令$\mathfrak{G}$是一个M-羣，并令$\{\mathfrak{K}_\alpha\}$是$\mathfrak{G}$里不变M-子羣的集合，能使 $\cap\mathfrak{K}_\alpha=1$。求証：$\mathfrak{G}$ 同构于羣 $\mathfrak{G}_\alpha=\mathfrak{G}/\mathfrak{K}_\alpha$ 的一个子直接积。

1）这是与直接积 Π 对应的加法方面的术語与記法．——著者注．

第 六 章

模 及 理 想

本章討論的模的概念是以环及带算子羣的概念为基础的一个合成概念. 模在研究抽象环到交換羣的自同态环内的同态（所謂表示論)时是非常重要的. 这点首先为諾德所認識;但这个概念以前在代数数論上已經出現.

本章第一部分引入模的基本概念,进一步考察模的鏈条件,及有关一般与特殊理想的希尔柏特(Hilbert)基条件. 第二部分是导出諾德环(带升鏈条件的交换环)里关于理想的基本分解定理. 最后,叙述整性相关的概念,第三章討論的代数相关的概念是它的特殊情形;因此,这里所述的各結論可应用于域論中.

1. 定义

定义 1. 左模是带有一个算子集合 $\mathfrak{A}$ 的交換羣 $\mathfrak{M}$(合成用加法),这里 $\mathfrak{A}$ 是一个环,而 $\mathfrak{M}$ 于适合基本算子条件

1_l. $$a(x+y)=ax+ay,\quad a\in\mathfrak{A},\quad x,y\in\mathfrak{M}$$

外,还适合

2_l. $$(a+b)x=ax+bx,$$

及

3_l. $$(ab)x=a(bx).$$

現在用記号 a_l 表示交換羣 $\mathfrak{M}$ 里的自同态 $x\to ax$, 则 2_l 及 3_l 两条件与关于这些自同态的下面两条件:

$2_l'$. $$(a+b)_l=a_l+b_l,$$

$3_l'$. $$(ab)_l=b_la_l$$

是等价的. 故知映照 $a\to a_l$ 是 $\mathfrak{A}$ 到 $\mathfrak{M}$ 的自同态环内的一个反同态. 反过来,如果 $\mathfrak{M}$ 是一个交換羣以环 $\mathfrak{A}$ 作为算子集合,而映

照 $a \to a_l$ 是一个反同态，则 $\mathfrak{M}$ 是一个左 $\mathfrak{A}$-模.

我們知道，从条件 1 可推得

(1) $$a0 = 0, \quad a(-x) = -ax.$$

又因为 $a \to a_l$ 是一个反同态，所以，$0_l = 0$，并且 $(-a)_l = -a_l$. 故

(2) $$0x = 0, \quad (-a)x = -ax.$$

仿此可定义右模的概念. 它是带有算子集合 $\mathfrak{A}$ 的一个交换羣 $\mathfrak{M}$，$\mathfrak{A}$ 是一个环，并且假定 $a \in \mathfrak{A}$ 映到 $\mathfrak{M}$ 里与 a 相連的自同态的映照是一种环同态. 为方便計，与 a 相連的自同态記作 a_r，并以 xa 表示 $a \in \mathfrak{A}$ 与 $x \in \mathfrak{M}$ 的积；于是，$xa_r = xa$. 关于这个积的假定是：

1_r. $$(x+y)a = xa + ya,$$

2_r. $$x(a+b) = xa + xb,$$

3_r. $$x(ab) = (xa)b.$$

如果 $\mathfrak{A}$ 是一个交换环，则 $\mathfrak{A}$ 的任一个同态也是一个反同态；反过来也是眞的. 所以，对于这样环的任一个左模可看作一个右模；反过来也是眞的. 这在任意环的情形不能成立. 但如果 $\mathfrak{A}$ 是一个任意环，而 $\mathfrak{A}'$ 是与 $\mathfrak{A}$ 反同构的一个环，则任一个左(右) $\mathfrak{A}$-模可看作一个右(左) $\mathfrak{A}'$-模. 为着这个目的，我們可命 $xa' = ax$ $(a'x = xa)$，这里 $a \to a'$ 是 $\mathfrak{A}$ 到 $\mathfrak{A}'$ 上的一个反同构. 于是，对应 $a' \to a_l (a' \to a_r)$ 显然是所求的 $\mathfrak{A}'$ 的一个同态(反同态).

一个环的加法羣当然可用为那些带算子羣里羣的部分. 我們先取环 $\mathfrak{A}$ 里的 a 与加法羣 $\mathfrak{M} = \mathfrak{A}, +$ 里的 x 的积为环的积 ax，显然 2_l 及 3_l 都成立. 于是，这个带算子羣就是一个左模. 此后，这种模叫做环 $\mathfrak{A}$ 的左模. 仿此，取 $\mathfrak{M} = \mathfrak{A}, +$ 而定义 $x \in \mathfrak{M}$ 与 $a \in \mathfrak{A}$ 的积为环的积 xa，这样就得环 $\mathfrak{A}$ 的右模.

2. 基本概念 此后我們只就左模来討論，而仅叫它做"模"，或"$\mathfrak{A}$-模". 显然对于左模有什么結果，在右模也有相应的結果.

令 $\mathfrak{M}$ 是一个 $\mathfrak{A}$-模，并令 $\mathfrak{N}$ 是 $\mathfrak{M}$ 的一个 $\mathfrak{A}$-子羣；这就是說，$\mathfrak{N}$ 是 $\mathfrak{M}$ 的一个子羣，并且 $\mathfrak{N}$ 对于与 $\mathfrak{A}$ 的元素作的乘法是封閉的. 于是积 $ay (a \in \mathfrak{A}, y \in \mathfrak{N})$ 显然适合 2_l 及 3_l. 故 $\mathfrak{N}$ 是一个模. 这种模叫做 $\mathfrak{M}$ 的一个子模.

設 $\mathfrak{N}$ 是 $\mathfrak{M}$ 的一个子模，则商羣 $\mathfrak{M}/\mathfrak{N}$ 可由規定

$$a(x+\mathfrak{N})=ax+\mathfrak{N}$$

而成为一个 $\mathfrak{A}$-羣．由此又可見，这个合成定义一个模，这个模叫做 $\mathfrak{M}$ 关于 $\mathfrak{N}$ 的差模．由于我們此后常同时討論差环与差模，故为方便起見，对于記号采取了下面的規定：即仍以 $\mathfrak{A}/\mathfrak{B}$ 表差环，而以 $\mathfrak{M}-\mathfrak{N}$ 表差模．

$\mathfrak{A}$-模的同态、同构、自同态及自同构各概念是带算子羣方面这些概念的特殊情形．故对于带算子羣方面这些概念所得出的結果无須改变即可轉移于模．例如，我們有：在同态 η 下，一个模 $\mathfrak{M}$ 的象 $\mathfrak{M}\eta$ 是一个子模．这个映照的核 $\mathfrak{K}$ 是 $\mathfrak{M}$ 的一个子模，并得"基本定理"：$\mathfrak{M}\eta\cong\mathfrak{M}-\mathfrak{K}$．再則环 $\mathfrak{A}$ 的左模的子模即是左理想 $\mathfrak{J}$．

这些观念的重要应用是模 $\mathfrak{M}$ 里一个元素的阶理想的定义．令 x 是 $\mathfrak{M}$ 的任一个元素，而考究 $\mathfrak{A}$ 到 $\mathfrak{M}$ 内的映照 $a\rightarrow ax$．显然，这是一个羣同态．又因为

(3) $$ba\rightarrow(ba)x=b(ax),$$

所以是一个 $\mathfrak{A}$-同态．于是，可得下面的結論：象 ax 的集合 $\mathfrak{A}x$ 是 $\mathfrak{M}$ 的一个子模，并且映照的核 $\mathfrak{J}_x$ 是环 $\mathfrak{A}$ 的一个左理想(子模)．由定义知，$\mathfrak{J}_x$ 是 $\mathfrak{A}$ 里元素 c 的集合，它使 $cx=0$ 的．这个理想叫做元素 x 的阶理想．由基本定理知，$\mathfrak{A}x\cong\mathfrak{A}-\mathfrak{J}_x$．

次考究 $\mathfrak{A}$ 到 $\mathfrak{M}$ 的自同态环内的环反同态 $a\rightarrow a_l$ 的核 $\mathfrak{Z}$．集合 $\mathfrak{Z}$ 显然是 $\mathfrak{M}$ 的元素的所有阶理想的交 $\cap\mathfrak{J}_x$．象元素 a_l 的子环 $\mathfrak{A}_l$ 是与 $\mathfrak{A}/\mathfrak{Z}$ 反同构的．这 $\mathfrak{Z}$ 叫做模 $\mathfrak{M}$ 的零化子，并为方便計記作 $0:\mathfrak{M}$．

一般說来，如果 $\mathfrak{N}_1$ 及 $\mathfrak{N}_2$ 是 $\mathfrak{M}$ 的两个子模，则 $\mathfrak{A}$ 的元素 c 能使

(4) $$c\mathfrak{N}_2\subseteq\mathfrak{N}_1$$

时，c 的集合記作 $\mathfrak{N}_1:\mathfrak{N}_2$．显然 $\mathfrak{N}_1:\mathfrak{N}_2$ 是 $\mathfrak{A}$ 里一个(双側)理想．这个理想叫做 $\mathfrak{N}_2$ 除 $\mathfrak{N}_1$ 的商．将来可見，商理想的研究在交換环的理想論上是非常重要的．

如果 $\mathfrak{B}$ 是环 $\mathfrak{A}$ 的一个子环，显然任一个 $\mathfrak{A}$-模可作为一个 $\mathfrak{B}$ 模．次假定 $\mathfrak{M}$ 是一个 $\mathfrak{A}$ 模，而 $\mathfrak{U}$ 是 $\mathfrak{A}$ 里一个理想含于 $0:\mathfrak{M}$ 里．

今将証明$\mathfrak{M}$也是一个 $\mathfrak{A}/\mathfrak{U}$-模. 这因为，令 a_1 及 a_2 是$\mathfrak{A}$里任意两个元素，它們属于同一个陪集 mod$\mathfrak{U}$, 則 $a_2 = a_1 + u$, $u \in \mathfrak{U}$. 于是，对于$\mathfrak{M}$里任一个 x 得 $a_2x = a_1x + ux = a_1x$. 由此知，以

$$(a + \mathfrak{U})x = ax \tag{5}$$

定义的积是 $\mathfrak{A}/\mathfrak{U} \times \mathfrak{M}$ 到$\mathfrak{M}$内的单值映照. 我們还可直接驗証：这个合成适合 1_l, 2_l 及 3_l. 因此就得一个 $\mathfrak{A}/\mathfrak{U}$-模.

习 题 62

1. 如果 $\mathfrak{J}$ 是 $\mathfrak{A}$ 的一个左理想，令 $\mathfrak{J}\mathfrak{M}$ 表示有限和 Σb_ix_i 的集合，这里 $b_i \in \mathfrak{J}$, $x_i \in \mathfrak{M}$. 求証：$\mathfrak{J}\mathfrak{M}$ 是 $\mathfrak{M}$ 的一个子模.

2. 如果 $\mathfrak{J}$ 是 $\mathfrak{A}$ 的一个右理想，求証：对于 $\mathfrak{J}$ 里所有 b 能使 $by = 0$ 的元素 $y(\in \mathfrak{M})$ 的全体是一个子模.

3. 令 $\mathfrak{A}$ 是带恆等元素 1 的环，求証：任一个 $\mathfrak{A}$-模可有一个表示 $\mathfrak{M} = 1\mathfrak{M} \oplus \mathfrak{N}$, 这里 $1\mathfrak{M}$ 是元素 $1x$ 的子模，而 $\mathfrak{N}$ 是被$\mathfrak{A}$里每个 a 所零化的元素构成的子模.

4. 整数环里下面的商：

$$(6):(3),\ (6):(15),\ (3):(9)$$

是什么？

5. 証明：关于商的下面法則：

(a) 如果 $\mathfrak{N}_1 \supseteq \mathfrak{N}_2$, 則 $\mathfrak{N}_1:\mathfrak{N}_2 = \mathfrak{A}$;

(b) $(\mathfrak{N}_1 \cap \mathfrak{N}_2 \cap \cdots \cap \mathfrak{N}_k):\mathfrak{N} = \mathfrak{N}_1:\mathfrak{N} \cap \mathfrak{N}_2:\mathfrak{N} \cap \cdots \cap \mathfrak{N}_k:\mathfrak{N}$;

(c) $\mathfrak{N}_1:\mathfrak{N}_2 = \mathfrak{N}_1:(\mathfrak{N}_1 + \mathfrak{N}_2)$.

6. 如果 $\mathfrak{N}_1 \subseteq \mathfrak{N}_2$, 則 $\mathfrak{N}_1:\mathfrak{N}_2 = 0:(\mathfrak{N}_2 - \mathfrak{N}_1)$.

7. 如果 $\mathfrak{A}$ 是带恆等元素环，求証：$\mathfrak{J}:\mathfrak{A}$ 是含在左理想 $\mathfrak{J}$ 里的 $\mathfrak{A}$ 的最大双側理想.

3. 生成元素. 单式模 如果X是模$\mathfrak{M}$的一个子集合，则形状如

$$m_1x_1 + m_2x_2 + \cdots + m_rx_r + a_1x_1 + a_2x_2 + \cdots + a_rx_r \tag{6}$$

的元素的集合(X)是$\mathfrak{M}$的一个子模，这里 m_i 是整数，$a_i \in \mathfrak{A}$, $x_i \in X$. 显然$(X) \supseteq X$. 并且$\mathfrak{M}$里包含着X的每个子模都含有(X)，故(X)叫做由X生成的子模 如果 $(X) = \mathfrak{M}$, 則説X是$\mathfrak{M}$的生成元素集合. 如果$\mathfrak{M}$里存在一个生成元素的有限集合，則$\mathfrak{M}$叫做一个有限生成模. 如果只有一个生成元素，則$\mathfrak{M}$是一个循环模.

公式(6)显示出一个元素对于生成元素集合的相关性，其中含有整数为系数的 m_i 及环 $\mathfrak{A}$ 的元为系数的 a_i, 頗为繁杂. 但在特殊情形，如果 $\mathfrak{A}\mathfrak{M} = \mathfrak{M}$, 亦即$\mathfrak{M}$的每个元素可写成形状 $\sum a_iy_i$, 这里 $a_i \in \mathfrak{A}$, $y_i \in \mathfrak{M}$, 則$\mathfrak{M}$叫做单式模，此时公式就較簡单. 今証下面的

定理 1. 如果X是单式模 $\mathfrak{M}$ 的生成元素集合，則$\mathfrak{M}$的每个元素可寫成形狀

(7) $$a_1x_1 + a_2x_2 + \cdots + a_rx_r,$$

这里 $a_i \in \mathfrak{A}$，而 $x_i \in X$.

証　令 x 是 $\mathfrak{M}$ 的任一个元素，則有适宜的 $a_i \in \mathfrak{A}$ 与 $y_i \in \mathfrak{M}$，使 $x = \sum a_i y_i$. 于是，X 里存在有元素 x_j 使

$$y_i = \sum m_{ij}x_j + \sum a_{ij}x_j, m_{ij} \in I, a_{ij} \in \mathfrak{A}.$$

故

$$x = \sum a_i y_i = \sum m_{ij}a_i x_j + \sum a_i a_{ij} x_j = \sum b_j x_j,\ b_j = \sum_i m_{ij}a_i + \sum_i a_i a_{ij}.$$

在特款可知，如果 $\mathfrak{M}$ 是单式循环模，則 $\mathfrak{M}$ 含有一个元素 x，使 $\mathfrak{M}$ 的每个元素是 x 的倍数 ax. 特別是 $\mathfrak{A}$ 里有一个适宜元素 e 使 x 有 ex 形狀. 如果 $\mathfrak{M}$ 是单式模，而 $\mathfrak{A}$ 有恆等元素 1，則 1 对于$\mathfrak{M}$有恆等算子的作用；这因为，如果 $x = \sum a_i y_i$，則

$$1x = 1(\sum a_i y_i) = \sum (1a_i) y_i = \sum a_i y_i = x.$$

反过来，如果 1 作为恆等算子，显然任一个 x 可写成形狀$1x$. 故$\mathfrak{M}$是单式模. 所以，如果 $\mathfrak{A}$ 有恆等元素，則$\mathfrak{M}$是单式模的条件与 1_l是$\mathfrak{M}$里恆等映照的条件等价.

基环 $\mathfrak{A}$ 是一个除环时的单式模叫做向量空間. 它的詳細討論是本书第二册的主要內容.

习　題　63

1. 如果 $\mathfrak{J}$ 是左理想，而有一个元素 e 存在使 $xe \equiv x(\mathrm{mod}\,\mathfrak{J})$ 对于 $\mathfrak{A}$ 里所有 x 成立，則 $\mathfrak{J}$ 叫做正則左理想. 如果 $\mathfrak{M}$ 是一个单式循环模，求証：$\mathfrak{M} \cong \mathfrak{A} - \mathfrak{J}$，这里 $\mathfrak{J}$ 是一个适宜的正則左理想.

2. 如果 $\mathfrak{J}$ 是正則的，求証：$\mathfrak{J} \supseteq \mathfrak{J}:\mathfrak{A}$.

3. 令 $\mathfrak{M}$ 是一个单純 $\mathfrak{A}$-模. 求証：或者 $\mathfrak{A}\mathfrak{M} = 0$，这时 $\mathfrak{M}$ 是有限模，所含元素的个数是素数；或者 $\mathfrak{M}$是一个单式循环模，以非零元素为生成元素. 求証它的逆定理：如果这两个条件中有一个成立，則 $\mathfrak{M}$ 是单純模(注記：本題的第一部分是习題 35 的第一題的拓广).

4. 鏈条件　于带算子羣中曾引入的鏈条件在模及理想論的各方面也居于一个重要角色. 我們即将知道（下一节），域上多項式环里的理想适合升鏈条件，并且单是这事实就足够引出这种环的

基理想的分解定理．另一方面，如果环适合关于理想的降鏈条件，这种环的研究成为环的結构論的一个重要部分．

本节及次节将引出鏈条件的若干簡单推論．因为任一个模都是一个交换羣，所以关于模的鏈条件可述之如次：

降鏈条件　如果 $\mathfrak{N}_1 \supseteq \mathfrak{N}_2 \supseteq \cdots$ 是子模的一个递降序列，則有一个整数 N 存在，使 $\mathfrak{N}_N = \mathfrak{N}_{N+1} = \cdots$．

升鏈条件　如果 $\mathfrak{N}_1 \subseteq \mathfrak{N}_2 \subseteq \cdots$ 是子模的一个递升序列，則有一个整数 N 存在，使 $\mathfrak{N}_N = \mathfrak{N}_{N+1} = \cdots$．

我們易知(使用选择公理[1])，降鏈条件等价于

极小条件　在任一个非空的子模集合 $\{\mathfrak{N}\}$ 里必存在着一个极小子模，亦即存在有一个子模使这个集合里任一个子模都不是它的眞子模．

要証明它們的等价关系，先假定降鏈条件成立．令 $\{\mathfrak{N}\}$ 是子模的一个非空集合．在这个集合里选取 $\mathfrak{N}_1$，則 $\mathfrak{N}_1$ 或者就是极小的，或者于 $\{\mathfrak{N}\}$ 里有 $\mathfrak{N}_2$ 存在，使 $\mathfrak{N}_2 \subset \mathfrak{N}_1$．在后者情形下，或者 $\mathfrak{N}_2$ 是极小的，或者于 $\{\mathfrak{N}\}$ 里有 $\mathfrak{N}_3$ 存在，使 $\mathfrak{N}_3 \subset \mathfrak{N}_2$．这样进行了有限次后，必达到一个极小子模；否則，由选择公理可得一个无限鏈 $\mathfrak{N}_1 \supset \mathfrak{N}_2 \supset \cdots$，这与假設矛盾．反过来，假設极小条件成立，并令 $\mathfrak{N}_1 \supseteq \mathfrak{N}_2 \supseteq \cdots$ 是子模的一个无限递降序列．令 $\mathfrak{N}_N$ 是集合 $\{\mathfrak{N}\}$ 里一个极小元素，則有 $\mathfrak{N}_N = \mathfrak{N}_{N+1} = \cdots$．

仿此可証升鏈条件等价于

极大条件　在任一个非空的子模集合里必存在着一个极大子模，亦即存在有一个子模使它不是这个集合里任一个子模的眞子模．

极大条件可推出下面有用的归納法原理：令 P 是一个模的子模的一个性质．当每个 $\mathfrak{N}' \supset \mathfrak{N}$ 时，如果 $P(\mathfrak{N}')$ 成立即可确定 $P(\mathfrak{N})$

1）設 S 是一个非空集合．令 $\mathfrak{T}$ 是 S 的所有子集合的集合，空集除外．令 ϕ 是 $\mathfrak{T}$ 到 S 上的一个映照，它使 S 的每个子集合 T 都与 S 的一个元素 $x = \phi(T)$ 相伴．如果 $\phi(T) \in T$，則 ϕ 叫做 S 的选择函数．选择公理是：每个集合有一个选择函数．

我們对于集合有这样的問題：在什么集合里可定义一个次序关系使这个集合是良序呢？由这公理可推得澤默路(Zelmelo)定理：每个集合都可以良序，因而解决了上面的問題——譯者註．

也成立，则$P(\mathfrak{N})$对于所有$\mathfrak{N}$都成立．这原理的証明与关于自然数的归納法原理的証明(引論的§4)相似；可直接由考究使$P(\mathfrak{N})$不成立的子模$\mathfrak{N}$的集合而得出．

我們即将导出的下面結果在理想論上是极有用的．今述之如次：

定理 2. 一个模$\mathfrak{M}$能适合关于子模的升鏈条件必須而且只須$\mathfrak{M}$的每个子模是有限生成的．

証 先設升鏈条件成立，并令$\mathfrak{N}$是$\mathfrak{M}$的任一个子模．如果$\mathfrak{N}=0$，則$\mathfrak{N}$由0生成．如果$\mathfrak{N}\neq 0$，令u_1是$\mathfrak{N}$的任一个非零元素，并令(u_1)表示由u_1生成的子模．如果$(u_1)\subset\mathfrak{N}$，令$u_2\in\mathfrak{N}$，但$\notin(u_1)$，則$(u_1)\subset(u_1,u_2)$，这里(u_1,u_2)是由u_1及u_2生成的子模．如果$(u_1,u_2)\subset\mathfrak{N}$，則可于$\mathfrak{N}$里选出$u_3$，使$(u_1,u_2,u_3)\supset(u_1,u_2)$．經有限次选取后，必得$(u_1,u_2,\cdots,u_n)=\mathfrak{N}$；否則，将得子模的无限眞升鏈$(u_1)\subset(u_1,u_2)\subset(u_1,u_2,u_3)\subset\cdots$，而与假設矛盾．

次設任一个子模都是有限生成的，并且令$\mathfrak{N}_1\subseteq\mathfrak{N}_2\subseteq\mathfrak{N}_3\subseteq\cdots$是子模的一个任意升鏈，則关于存在整数$N$使$\mathfrak{N}_N=\mathfrak{N}_{N+1}=\cdots$的証明与关于主理想整区的升鏈条件的証明(第四章的§4)相似．如象在特殊情形，我們注意到邏輯和$\mathfrak{P}=\bigcup\mathfrak{N}_i$是一个子模．故$\mathfrak{P}$里有适宜的$u_i$使$\mathfrak{P}=(u_1,u_2,\cdots,u_r)$．于是有$h_i$使$u_i\in\mathfrak{N}_{h_i}$．如果$N=\max(h_1,h_2,\cdots,h_r)$，則每个$u_i\in\mathfrak{N}_N$．于是，$\mathfrak{P}\subseteq\mathfrak{N}_N$，并且显然可推得$\mathfrak{N}_N=\mathfrak{N}_{N+1}=\cdots$．

5. 希尔柏特的基定理 今設$\mathfrak{M}$是一个有限生成的单式模．我們将証：如果环$\mathfrak{A}$适合左理想的升(降)鏈条件，則这条件对于$\mathfrak{M}$也成立．

令$x_1,x_2,\cdots,x_r$是$\mathfrak{M}$的生成元素的一个固定集合．如果$\mathfrak{N}$是$\mathfrak{M}$的任一个子模，而$\mathfrak{A}$里的元素b能使$\mathfrak{N}$里存在着一个元素

$$bx_j+b_{j+1}x_{j+1}+\cdots+b_rx_r$$

时，这样b的全体記作$\mathfrak{J}_j(\mathfrak{N})(j=1,2,\cdots,r)$．我們易知，$\mathfrak{J}_j(\mathfrak{N})$是一个左理想，而且如果$\mathfrak{N}\subseteq$子模$\mathfrak{P}$，显然有$\mathfrak{J}_j(\mathfrak{N})\subseteq\mathfrak{J}_j(\mathfrak{P})$．今証下面的引理．

引理 1. 如果 $\mathfrak{N}\subseteq\mathfrak{P}$，並且对于所有 j，$\mathfrak{J}_j(\mathfrak{N})=\mathfrak{J}_j(\mathfrak{P})$，則 $\mathfrak{N}=\mathfrak{P}$.

証 令 $y=b_1x_1+b_2x_2+\cdots+b_rx_r$ 是 $\mathfrak{P}$ 的任一个元素，則 $b_1\in\mathfrak{J}_1(\mathfrak{P})=\mathfrak{J}_1(\mathfrak{N})$. 故$\mathfrak{N}$里有形状如 $b_1x_1+b_2'x_2+\cdots+b_r'x_r$ 的一个元素 y' 存在. 于是，$y-y'=c_2x_2+c_3x_3+\cdots+c_rx_r$，这里 $c_i=b_i-b_i'$，而 $y-y'\in\mathfrak{P}$. 故 $c_2\in\mathfrak{J}_2(\mathfrak{P})=\mathfrak{J}_2(\mathfrak{N})$. 但，$\mathfrak{N}$ 里有形状如 $c_2x_2+c_3'x_3+\cdots+c_r'x_r$ 的一个元素 y'' 存在. 于是 $y-y'-y''=d_3x_3+\cdots+d_rx_r$. 这样継續下去，我們于 $\mathfrak{N}$ 里得 $y',y'',\cdots,y^{(r)}$，使 $y-y'-y''-\cdots-y^{(r)}=0$. 故 $y=y'+y''+\cdots+y^{(r)}\in\mathfrak{N}$.

今命 $\mathfrak{N}_1\subseteq\mathfrak{N}_2\subseteq\cdots$是 $\mathfrak{M}$ 的子模的一个升鏈，則伴着这个鏈可得 r 个左理想鏈

$$\mathfrak{J}_j(\mathfrak{N}_1)\subseteq\mathfrak{J}_j(\mathfrak{N}_2)\subseteq\cdots(j=1,2,\cdots,r).$$

如果升鏈条件在 $\mathfrak{A}$ 里成立，則对于每个 j 可得一个整数 N_j，使

$$\mathfrak{J}_j(\mathfrak{N}_{N_j})=\mathfrak{J}_j(\mathfrak{N}_{N_j+1})=\cdots(j=1,2,\cdots,r).$$

所以，如果 $N=\max(N_1,N_2,\cdots,N_r)$，則 $\mathfrak{J}_j(\mathfrak{N}_N)=\mathfrak{J}_j(\mathfrak{N}_{N+1})=\cdots(j=1,2,\cdots,r)$. 由引理 1 即可推得$\mathfrak{N}_N=\mathfrak{N}_{N+1}=\cdots$. 这証明了下面定理里关于升鏈的情形.

定理 3. 如果$\mathfrak{A}$是一个环，适合关于左理想的升(降)鏈条件，則任一个有限生成的單式$\mathfrak{A}$模$\mathfrak{M}$适合关于子模的升(降)鏈条件.

这定理关于降鏈情形的証明与上面的証法相似，不再贅述.

其次，我們要証：如果 $\mathfrak{A}$ 是一个带恆等元素的环，它适合升鏈条件，这等价于說：如果$\mathfrak{A}$里每个左理想是有限生成的，則同一条件对于含超越元素 x 的多項式环 $\mathfrak{A}[x]$ 也成立；这个結果的証明与前面証明十分相似.

对于 $\mathfrak{A}[x]$的每个左理想 $\mathfrak{N}$ 及每个 $j=0,1,2,\cdots$，伴着有 $\mathfrak{A}$ 里元素 b 的集合 $\mathfrak{J}_j(\mathfrak{N})$，使 $\mathfrak{N}$ 里存在有元素

$$bx^j+b_{j-1}x^{j-1}+\cdots+b_0.$$

显然$\mathfrak{J}_j(\mathfrak{N})$是 $\mathfrak{A}$ 里一个左理想. 又因为 $bx^j+b_{j-1}x^{j-1}+\cdots+b_0\in\mathfrak{N}$，則

$$bx^{j+1} + b_{j-1}x^j + \cdots + b_0x = x(bx^j + b_{j-1}x^{j-1} + \cdots + b_0) \in \mathfrak{N}.$$

于是，

$$\mathfrak{J}_0(\mathfrak{N}) \subseteq \mathfrak{J}_1(\mathfrak{N}) \subseteq \mathfrak{J}_2(\mathfrak{N}) \subseteq \cdots.$$

故集合 $\mathfrak{J}(\mathfrak{N}) = \bigcup \mathfrak{J}_j(\mathfrak{N})$ 是一个左理想．今将应用这些註記来証明重要的

希尔柏特的基定理 令 $\mathfrak{A}$ 是带恆等元素环，它的各个左理想都是有限生成的，则含超越元素 x 的多项式环 $\mathfrak{A}[x]$ 的各个左理想也都是有限生成的．

証 令 $\mathfrak{N}$ 是一个理想，并且定义理想 $\mathfrak{J}_j(\mathfrak{N})$ 及 $\mathfrak{J}(\mathfrak{N})$ 如前．则有一个整数 N，使 $\mathfrak{J}_N(\mathfrak{N}) = \mathfrak{J}_{N+1}(\mathfrak{N}) = \cdots = \mathfrak{J}(\mathfrak{N})$．令

$$b_{ji}(j = 0,1,2,\cdots,N; i = 1,2,\cdots,m_j)$$

是 $\mathfrak{A}$ 的元素，使

$$\mathfrak{J}_j(\mathfrak{N}) = (b_{j1}, b_{j2}, \cdots, b_{jm_j}),$$

并令 $f_{ji}(x)$ 是 $\mathfrak{N}$ 里多項式使

$$f_{ji}(x) = b_{ji}x^j + c_{ji}x^{j-1} + d_{ji}x^{j-2} + \cdots.$$

我們将証：

$$\mathfrak{N} = (f_{01}, \cdots, f_{0m_0}; f_{11}, \cdots, f_{1m_1}; \cdots; \cdots; f_{N,m_N}).$$

今令 $g = c_rx^r + c_{r-1}x^{r-1} + \cdots + c_0 \in \mathfrak{N}$．如果 $r \leqslant N$，则 $\mathfrak{A}$ 里有适宜的 a_{ri} 使 $c_r = a_{r1}b_{r1} + a_{r2}b_{r2} + \cdots + a_{rm_r}b_{rm_r}$；于是，$g - \sum a_{ri}f_{ri}(x)$ 是 $\mathfrak{N}$ 里一个多项式，它的次数 $< r$．如果 $r > N$，则 $\mathfrak{A}$ 里有适宜的 a_{ri} 使 $c_r = a_{r1}b_{N1} + a_{r2}b_{N2} + \cdots + a_{rm_N}b_{Nm_N}$；于是，$g - \sum a_{ri}x^{r-N}f_{Ni}(x)$ 是 $\mathfrak{N}$ 里一个多項式，它的次数 $< r$．故由对于 g 的次数施行归納法，即可获得所求結果．

希尔柏特的定理立可扩张于多元多項式，其結果如次：

系 1 令 $\mathfrak{A}$ 是带恆等元素环，並且 $\mathfrak{A}$ 里每个左理想都是有限生成的，则 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ 里每个左理想有有限生成元素．

这結果的一个重要特款是：

系 2 如果 $\mathfrak{A}$ 是一个除环，或是一个主理想整区，则 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ 的每个左(右)理想有一个有限的生成元素集合．

习 題 64

1．如果只就升鏈条件而論，求証：定理 3 里关于 $\mathfrak{M}$ 是单式模的假定是多余的．

2. 如果 $\mathfrak{A}$ 带有恆等元素，并且 $\mathfrak{A}$ 的各个左理想是有限生成的. 求証：环 $\mathfrak{A}$ 上 x 的冪級数环 $\mathfrak{A}\langle x\rangle$ （参看习題 39 的第 1 題）里各个左理想是有限生成的.

3. 令 $\mathfrak{F}$ 是含有 q 个元素的一个有限域，并令 $\mathfrak{Z}$ 是 $\mathfrak{F}[x_1,x_2,\cdots,x_r]$ 里多項式 $m(x_1,x_2,\cdots,x_r)$ 的理想，它对于 $\mathfrak{F}$ 里所有 s_i 使 $m(s_1,\cdots,s_r)=0$. 求决定 $\mathfrak{Z}$ 的生成元素所成的有限集合.

6. 諾德环．素理想及准素理想 在后数节里将闡述带升鏈条件的交換环的理想論上的基本結果. 我們已知，这种环包括着多項式环 $\mathfrak{F}[x_1,x_2,\cdots,x_r]$，这里 $\mathfrak{F}$ 是一个域. 多項式理想論是代数几何学的基础，而这个理論在仅以升鏈条件及交換性为基础的抽象发展是由諾德开端的. 因此，适合这两个条件的环叫做**諾德环**.

我們先假定 $\mathfrak{A}$ 是交換环，則在主理想整区的情形下可知：元素 d 是元素 b 的因子必須而且只須理想 $(d)\supseteq(b)$. 因此，如果 $\mathfrak{D}$ 及 $\mathfrak{B}$ 是任一个交換环的理想，而 $\mathfrak{D}\supseteq\mathfrak{B}$，則說：$\mathfrak{D}$ 是 $\mathfrak{B}$ 的一个**因子**，而 $\mathfrak{B}$ 是 $\mathfrak{D}$ 的一个**倍理想**. 仿此，由主理想情形引起我們把 $\mathfrak{B}_1+\mathfrak{B}_2$ 叫做 $\mathfrak{B}_1$ 与 $\mathfrak{B}_2$ 的**最大公因子**，而把 $\mathfrak{B}_1\cap\mathfrak{B}_2$ 叫做 $\mathfrak{B}_1$ 与 $\mathfrak{B}_2$ 的**最小公倍理想**. 这因为，在主理想整区里，$(b_1)+(b_2)=(d)$，这里 d 是 b_1 与 b_2 的最大公因子，而 $(b_1)\cap(b_2)=(m)$，这里 m 是 b_1 与 b_2 的最小公倍数. 其次是把素数概念扩张为下面重要的定义.

定义 2. 如果 $\mathfrak{B}$ 是交換环 $\mathfrak{A}$ 的一个理想，并且从 $ab\equiv0(\mathrm{mod}\,\mathfrak{B})$ 可推得 $a\equiv0(\mathrm{mod}\,\mathfrak{B})$ 或 $b\equiv0\ (\mathrm{mod}\,\mathfrak{B})$，則 $\mathfrak{B}$ 叫做**素理想**.

显然，这与 $\mathfrak{A}/\mathfrak{B}$ 成一个整区的条件等价. 我們也易知，$\mathfrak{A}$ 是整区必須而且只須 0 是一个素理想. 按第四章关于素数的定义知，元素 p 是素数必須而且只須 (p) 是一个素理想. 例如，$(x-y)$ 是 $\mathfrak{F}[x,y]$ 里素理想. 素理想但非主理想的一个例子是：$\mathfrak{F}[x,y]$ 里的理想 $(x,y)=(x)+(y)$. 此时，$\mathfrak{F}[x,y]/(x,y)\cong\mathfrak{F}$.

带恆等元素环里的任一个极大理想 $\mathfrak{B}$ 必是一个素理想；这因为，此时 $\mathfrak{A}/\mathfrak{B}$ 是一个域，因此也是一个整区. 如果 $\mathfrak{A}$ 不带恆等元素，而 $\mathfrak{B}$ 是极大理想，則或者 $\mathfrak{A}/\mathfrak{B}$ 是一个域，或者 $(\mathfrak{A}/\mathfrak{B})^2=0$. 在前一个情形，$\mathfrak{B}$ 是素理想，而在后一个情形，$\mathfrak{A}^2\subseteq\mathfrak{B}$.

次設 $\mathfrak{B}$ 是交換环 $\mathfrak{A}$ 里任一个理想，如果对于 $\mathfrak{A}$ 里的元素 z，有一个正整数 r 存在（可能与 z 有关）使 $z^r\equiv0(\mathrm{mod}\,\mathfrak{B})$，这样元素

z 的全体令为 $\mathfrak{R}=\mathfrak{R}(\mathfrak{B})$. 显然，$\mathfrak{R}$ 也可定义为元素 z 的集合能使陪集 $\bar{z}=z+\mathfrak{B}$ 在 $\mathfrak{A}/\mathfrak{B}$ 里是无势元素的. 今証明：$\mathfrak{R}$ 是一个理想. 首先，如果 $z^r\equiv 0(\bmod\mathfrak{B})$，并且 a 是 $\mathfrak{A}$ 的任一个元素，則有 $(az)^r=a^rz^r\equiv 0\ (\bmod\mathfrak{B})$. 其次，令 z_1 及 $z_2\in\mathfrak{R}$，并令 $z_i^{r_i}\equiv 0$ $(\bmod\mathfrak{B})(i=1,2)$. 因为

$$(z_1-z_2)^r=\sum m_{ij}z_1^iz_2^j,\quad i+j=r,\quad m_{ij}\in I,$$

故命 $r=r_1+r_2-1$，則右端每項有 $i\geqslant r_1$ 或 $j\geqslant r_2$，故 $m_{ij}z_1^iz_2^j\equiv 0(\bmod\mathfrak{B})$. 于是，$(z_1-z_2)^r\equiv 0(\bmod\mathfrak{B})$. 因此，$z_1-z_2\in\mathfrak{R}$. 故 $\mathfrak{R}$ 是理想. 我們叫它做 $\mathfrak{B}$ 的**根集**. 显然 $\mathfrak{R}$ 是 $\mathfrak{B}$ 的一个因子.

例 (1)令 $a=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$是整数 a 分解成素数的冪 $p_i^{e_i}$ 的积，这里 $i\neq j$ 时 $p_i\neq p_j$. 则(a)的根集是$(p_1p_2\cdots p_r)$. 这因为，如果 $b=kp_1p_2\cdots p_r$，而 $e=\max(e_1,e_2,\cdots,e_r)$，則 $b^e\equiv 0(\bmod(a))$. 反过来，如果 c 的冪可以 a 除尽，則 c 自身可以 $p_1p_2\cdots p_r$ 除尽. (2) 考究 $\mathfrak{J}[x,y]$ 里的理想 (x^2,y^3)，显然根集含有 x 及 y；另一方面，如果 $f(x,y)^r\equiv 0(\bmod(x^2,y^3))$，則 $f(x,y)$ 的常数項等于 0，故 $f(x,y)\equiv 0\ (\bmod(x,y))$. 因此，$(x^2,y^3)$的根集是$(x,y)$.

諾德环里每个理想 $\mathfrak{B}$ 的根集 $\mathfrak{R}$ 必是**无势的**$(\bmod\mathfrak{B})$，亦即必有一个整数N存在，使 $\mathfrak{R}^N\equiv 0(\bmod\mathfrak{B})$. 要証这結果，于 $\mathfrak{R}$ 里取由生成元素 $z_1,z_2,\cdots,z_m$ 所成的有限集合，使 $\mathfrak{R}=(z_1,z_2,\cdots,z_m)$. 令 r_i 是使 $z_i^{r_i}\equiv 0(\bmod\mathfrak{B})$的整数，并命 $N=r_1+r_2+\cdots+r_m-(m-1)$. 因为 $\mathfrak{R}$ 里任一个元素的形状是

$$\sum a_iz_i+\sum m_iz_i,\quad a_i\in\mathfrak{A},\quad m_i\in I,$$

故 $\mathfrak{R}$ 里任意N个元素的积的形状为

$$\sum A_{i_1\cdots i_m}z_1^{i_1}z_2^{i_2}\cdots z_m^{i_m}+\sum M_{i_1\cdots i_m}z_1^{i_1}z_2^{i_2}\cdots z_m^{i_m},$$

这里 $A_{i_1\cdots i_m}\in\mathfrak{A}$，而 $M_{i_1\cdots i_m}\in I$，并且 $i_1+i_2+\cdots+i_m=N$. 我們易知，每項里必有某个 j 使 $i_j\geqslant r_j$；因而这項就属于 $\mathfrak{B}$. 故 $\mathfrak{R}$ 里任意N个元素的积属于 $\mathfrak{B}$，从而推知 $\mathfrak{R}^N\equiv 0(\bmod\mathfrak{B})$.

次考究在主理想整区里素数冪元素的概念的拓广. 它可有种种的可能性，但就分解理論的目的来説，下面所給的重要定义是"正确"的一个.

定义 3. 令 $\mathfrak{B}$ 是交換环的一个理想，如果关于 $\bmod\mathfrak{B}$ 的每个零因子属于根集 $\mathfrak{R}$，亦即：如果 $ab\equiv 0(\bmod\mathfrak{B})$，及 $b\not\equiv 0(\bmod\mathfrak{B})$，

可推得 $a\equiv0(\mathrm{mod}\mathfrak{R})$，则 $\mathfrak{B}$ 叫做**准素理想**.

这个定义的直接推論是：一个准素理想的根集是一个素理想. 这因为，令 $ab\in\mathfrak{R}$ 并設 $a\not\equiv0\ (\mathrm{mod}\mathfrak{R})$，則有正整数 r 存在使 $a^rb^r=(ab)^r\equiv0(\mathrm{mod}\mathfrak{B})$. 另一方面，如果 $a^r\not\equiv0(\mathrm{mod}\mathfrak{B})$，則由定义，$b^r\equiv0\ (\mathrm{mod}\mathfrak{R})$；这意味着有整数 s 存在，使 $b^{rs}=(b^r)^s\equiv 0(\mathrm{mod}\mathfrak{B})$. 故 $b\in\mathfrak{R}$. 准素理想 $\mathfrak{B}$ 的根集叫做 $\mathfrak{B}$ 的**相伴素理想**.

我們易知，(q) 是整数环里的准素理想必須而且只須 $q=p^c$，这里 p 是一个素数(参看习题 65 的第 1 题). 理想 (x^2,y^3) 是 $\mathfrak{J}[x,y]$ 中的准素理想,这事实让讀者驗証. 另一方面，虽然理想 (x^2,xy) 的根集 (x) 是素理想，但 (x^2,xy) 不是 $\mathfrak{J}[x,y]$ 的准素理想；这因为，虽然 $x\not\equiv0(\mathrm{mod}(x^2,xy))$ 及 $y\not\equiv0(\mathrm{mod}(x))$，但是，$xy\equiv0(\mathrm{mod}\ (x^2,xy))$.

习　题　65

1. 如果 $q\neq0,1$，求証：(q) 是 I 的准素理想必須而且只須 $q=p^e$，这里 p 是一个素数.
2. 如果 $\mathfrak{B}$ 是一个素理想，并且 $\mathfrak{C}_1$ 及 $\mathfrak{C}_2$ 是使 $\mathfrak{C}_1\mathfrak{C}_2\equiv0(\mathrm{mod}\mathfrak{B})$ 的理想. 求証：$\mathfrak{C}_1\equiv0(\mathrm{mod}\mathfrak{B})$，或者 $\mathfrak{C}_2\equiv0(\mathrm{mod}\mathfrak{B})$.
3. 求証：$\mathfrak{R}(\mathfrak{B}_1\cap\mathfrak{B}_2)=\mathfrak{R}(\mathfrak{B}_1)\cap\mathfrak{R}(\mathfrak{B}_2)$.
4. 求証：$\mathfrak{B}_1^t\subseteq\mathfrak{B}_2$ 在一个諾德环里成立必須而且只須 $\mathfrak{R}(\mathfrak{B}_1)\subseteq\mathfrak{R}(\mathfrak{B}_2)$.

7. 理想分解为准素理想的交　整数环里因子分解的基本定理可借理想述之如次：每个理想 (a) 必有而且只有一种方法写成素理想的积. 这事实在任意諾德环是不成立的. 較弱一些的說法是：I 里每个理想是准素理想的交(最小公倍理想). 这因为，如果 $a=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$，这里 p_i 是不同的素数，則显然

$$(a)=(p_1^{e_1})\cap(p_2^{e_2})\cap\cdots\cap(p_r^{e_r}).$$

本节里将証明：这样表示在諾德环里成立. 唯一性問題則将于 §8 里討論.

設 $\mathfrak{A}$ 是任一个諾德环. 我們先証：非准素理想必是**可約的**，就是說，可写成眞因子的交. 这因为，設 $\mathfrak{B}$ 不是准素理想，并令 d 是一个元素，它是关于 $\mathrm{mod}\mathfrak{B}$ 的零因子，但 $\notin\mathfrak{R}(\mathfrak{B})$. 令 a 是一个元素，使 $ad\equiv0(\mathrm{mod}\mathfrak{B})$，并且 $a\not\equiv0(\mathrm{mod}\mathfrak{B})$. 則 $a\in\mathfrak{B}:(d)$，但 $\notin\mathfrak{B}$.

故 $\mathfrak{B}:(d)\supset\mathfrak{B}$. 又因为 $d\notin\mathfrak{R}(\mathfrak{B})$, 故 $(d^k)+\mathfrak{B}\supset\mathfrak{B}$ $(k=1,2,3,\cdots)$. 今考究升鏈

(8) $$\mathfrak{B}:(d)\subseteq\mathfrak{B}:(d^2)\subseteq\mathfrak{B}:(d^3)\subseteq\cdots.$$

令 r 是正整数使

(9) $$\mathfrak{B}:(d^r)=\mathfrak{B}:(d^{r+1})=\cdots,$$

则有关系

(10) $$\mathfrak{B}=(\mathfrak{B}:(d^r))\cap(\mathfrak{B}+(d^{r+1}));$$

这因为，如果 $u\in\mathfrak{B}+(d^{r+1})$，则 $u=b+md^{r+1}+cd^{r+1}$，这里 $b\in\mathfrak{B},m\in I,c\in\mathfrak{A}$. 所以，如果 $u\in\mathfrak{B}:(d^r)$，则

$$ud^r=bd^r+md^{2r+1}+cd^{2r+1}\equiv0(\mathrm{mod}\,\mathfrak{B}).$$

由此得 $(md+cd)d^{2r}\equiv0(\mathrm{mod}\,\mathfrak{B})$；于是，$md+cd\in\mathfrak{B}:(d^{2r})$. 但由(9)得 $(md+cd)d^r\equiv0(\mathrm{mod}\,\mathfrak{B})$，故 $md^{r+1}+cd^{r+1}\equiv0(\mathrm{mod}\,\mathfrak{B})$. 因此 $u\in\mathfrak{B}$，而(10)就被証明了. 因为(10)里两个理想都是 $\mathfrak{B}$ 的眞因子，故 $\mathfrak{B}$ 是可約的. 我們所証的結果显然可述成下面形状：

定理 4. 諾德环里每个不可約理想都是准素理想.

其次，我們来証明：諾德环里每个理想都是有限个不可約理想的交. 要証这个性质，我們使用 §4 里所述的归納法原理，亦卽：假定这个性质对于所有 $\mathfrak{B}_1\supset\mathfrak{B}$ 能成立，而証明它对于 $\mathfrak{B}$ 也成立. 这因为，如果 $\mathfrak{B}$ 是不可約的，就不必进行了；否則，$\mathfrak{B}=\mathfrak{B}_1\cap\mathfrak{B}_2$，这里 $\mathfrak{B}_i\supset\mathfrak{B}(i=1,2)$. 于是，因为 $\mathfrak{B}_1$ 及 $\mathfrak{B}_2$ 可由有限个不可約理想的交表出，从而 $\mathfrak{B}$ 也是有限个理想的交. 更由定理 4 就可推出下面的关于分解的基本定理：

定理 5. 諾德环里每个理想都是有限个准素理想的交.

习 题 66

1. 求把 (x^2,xy) 写成有限个准素理想的交.

2. 求証：理想 (x^2,xy,y^2) 是准素理想，并且在 $\mathfrak{J}[x,y]$ 里是可約的.

3. 求証費廷定理：令 $\mathfrak{M}$ 是一个 $\mathfrak{A}$-模 ($\mathfrak{A}$ 是任意的)，适合升鏈条件. 設有 $\mathfrak{M}$ 的一个 $\mathfrak{A}$-自同态 θ 存在，它不是无势的，也不是 $\mathfrak{M}$ 的一个同构. 則 $\mathfrak{M}$ 里存在有两个子模 $\mathfrak{M}_i\neq0(i=1,2)$，使 $\mathfrak{M}_1\cap\mathfrak{M}_2=0$.

4. 求証費廷定理：令 $\mathfrak{M}$ 是适合升鏈条件的一个 $\mathfrak{A}$-模. 設 $\mathfrak{M}$ 的任意两个非零模的交 $\neq0$. 則 $\mathfrak{M}$ 的无势 $\mathfrak{A}$-自同态的集合是 $\mathfrak{A}$-自同态环 $\mathfrak{E}$ 里一个理想 $\mathfrak{R}$. 如果 $\alpha\in\mathfrak{E}$ 是一个左零因子，則 $\alpha\in\mathfrak{R}$.

8. 唯一性定理 如果 $\mathfrak{Q}_1,\mathfrak{Q}_2,\cdots,\mathfrak{Q}_r$ 是理想，而理想

$$\mathfrak{B}=\mathfrak{Q}_1\cap\mathfrak{Q}_2\cap\cdots\cap\mathfrak{Q}_r,$$

并且

$$\mathfrak{Q}_1\cap\cdots\cap\mathfrak{Q}_{i-1}\cap\mathfrak{Q}_{i+1}\cap\cdots\cap\mathfrak{Q}_r\supset\mathfrak{B}(i=1,2,\cdots,r)$$

則說理想 $\mathfrak{B}$ 是理想 $\mathfrak{Q}_1,\mathfrak{Q}_2,\cdots,\mathfrak{Q}_r$ 的无贅交. 如果已得到用有限个理想的交作出的 $\mathfrak{B}$ 的一种表示，則显然可将多余的項去掉，以得一个无贅交. 在特款，我們知道，諾德环里每个理想是准素理想的一个无贅交. 其次，我們要証：准素理想有时可以合併仍得准素理想，这就是下面的

引理 1. 如果 $\mathfrak{Q}_1$ 及 $\mathfrak{Q}_2$ 是有相同根集 $\mathfrak{P}$ 的准素理想，則 $\mathfrak{Q}_1\cap\mathfrak{Q}_2$ 是准素理想.

証 因为 $\mathfrak{R}(\mathfrak{Q}_1\cap\mathfrak{Q}_2)=\mathfrak{R}(\mathfrak{Q}_1)\cap\mathfrak{R}(\mathfrak{Q}_2)$，故 $\mathfrak{R}(\mathfrak{Q}_1\cap\mathfrak{Q}_2)=\mathfrak{P}$. 今令 a 是关于 $\mathrm{mod}(\mathfrak{Q}_1\cap\mathfrak{Q}_2)$ 的一个零因子，則有一个 $b\not\equiv 0(\mathrm{mod}\mathfrak{Q}_1\cap\mathfrak{Q}_2)$ 使 $ab\equiv 0\ (\mathrm{mod}(\mathfrak{Q}_1\cap\mathfrak{Q}_2))$. 因为 $b\not\equiv 0\ (\mathrm{mod}(\mathfrak{Q}_1\cap\mathfrak{Q}_2))$，故可設 $b\not\equiv 0(\mathrm{mod}\mathfrak{Q}_1)$. 于是，从 $ab\equiv 0(\mathrm{mod}\mathfrak{Q}_1)$，得 $a\equiv 0(\mathrm{mod}\mathfrak{R}(\mathfrak{Q}_1))$，故 $a\in\mathfrak{P}$.

当一个表示的各項中遇有它們的相伴素理想相同时，则由引理 1 知，这样的項可以合併. 經过如此整理后，就得 $\mathfrak{B}$ 用准素理想的无贅交的一个表示

$$\mathfrak{B}=\mathfrak{Q}_1\cap\mathfrak{Q}_2\cap\cdots\cap\mathfrak{Q}_r, \tag{11}$$

这时它們的相伴素理想 $\mathfrak{P}_1,\mathfrak{P}_2,\cdots,\mathfrak{P}_r$ 各不相同. 但虽經这样正規化后，不能就肯定地說：$\mathfrak{Q}_i$ 是唯一的. 例如，(x^2,xy) 在 $\mathfrak{F}[x,y]$ 里有不同的分解：

$$\begin{aligned}(x^2,xy)&=(x)\cap(x^2,xy,y^2)\\&=(x)\cap(x^2,y+\alpha x),\quad \alpha\in\mathfrak{F}.\end{aligned}$$

但是这两个分解的相伴素理想，即 (x) 及 (x,y)，是相同的，并且这种統一性是一般成立的. 这便是后面第一唯一性定理的內容. 我們現在先导出两个簡单引理.

引理 2. 令 $\mathfrak{Q}$ 是准素理想，並令 $\mathfrak{P}'$ 是一个素理想，$\mathfrak{P}'\supseteq\mathfrak{Q}$，則 $\mathfrak{P}'\supseteq\mathfrak{P}=\mathfrak{R}(\mathfrak{Q})$.

証　如果 $z\equiv 0(\bmod \mathfrak{P})$，則有整数 r 使 $z^r\equiv 0(\bmod \mathfrak{Q})$. 于是，$z^r\equiv 0(\bmod \mathfrak{P}')$. 因为 $\mathfrak{P}'$ 是素理想，故 $z\equiv 0(\bmod \mathfrak{P}')$.

引理 3. 令 $\mathfrak{Q}$ 是准素理想，$\mathfrak{P}$ 是它的相伴素理想，並令 $\mathfrak{C}$ 是不含于 $\mathfrak{P}$ 里的任一个理想，則 $\mathfrak{Q}:\mathfrak{C}=\mathfrak{Q}$.

証　$\mathfrak{Q}:\mathfrak{C}$ 里一个元素 u 对于 $\mathfrak{C}$ 里所有 c 适合条件 $uc\equiv 0(\bmod \mathfrak{Q})$. 如果取 $c\not\equiv 0(\bmod \mathfrak{P})$，則可推得 $u\equiv 0(\bmod \mathfrak{Q})$. 于是，$\mathfrak{Q}:\mathfrak{C}\subseteq\mathfrak{Q}$. 显然 $\mathfrak{Q}\subseteq\mathfrak{Q}:\mathfrak{C}$. 故 $\mathfrak{Q}:\mathfrak{C}=\mathfrak{Q}$.

今来証明下面的定理.

第一唯一性定理　令 $\mathfrak{B}=\mathfrak{Q}_1\cap\mathfrak{Q}_2\cap\cdots\cap\mathfrak{Q}_r=\mathfrak{Q}'_1\cap\mathfrak{Q}'_2\cap\cdots\cap\mathfrak{Q}'_s$ 是两种准素理想的无贅交，每組准素理想的相伴素理想互不相同，則 $r=s$，并且两种分解的素理想的集合完全相同.

証　令 $\mathfrak{P}_i=\mathfrak{R}(\mathfrak{Q}_i)$，$\mathfrak{P}'_i=\mathfrak{R}(\mathfrak{Q}'_i)$，則在 $\mathfrak{P}_1,\mathfrak{P}_2,\cdots,\mathfrak{P}_r,\mathfrak{P}'_1,\mathfrak{P}'_2,\cdots,\mathfrak{P}'_s$ 的集合里有理想存在，使这个集合里任一个理想都不眞含着它們. 今假定 $\mathfrak{P}_1$ 具有这个性质. 我們先証 $\mathfrak{P}_1$ 必在 $\mathfrak{P}'_1,\mathfrak{P}'_2,\cdots,\mathfrak{P}'_s$ 的集合里. 否則，$\mathfrak{P}_1\neq\mathfrak{P}'_i(i=1,2,\cdots,s)$. 于是，由引理 2 知，$\mathfrak{Q}_1\not\subseteq\mathfrak{P}'_i$. 故由引理 3 知，$\mathfrak{Q}'_i:\mathfrak{Q}_1=\mathfrak{Q}'_i$. 于是，

$$\begin{aligned}\mathfrak{B}:\mathfrak{Q}_1&=(\mathfrak{Q}'_1\cap\mathfrak{Q}'_2\cap\cdots\cap\mathfrak{Q}'_s):\mathfrak{Q}_1\\&=\mathfrak{Q}'_1:\mathfrak{Q}_1\cap\mathfrak{Q}'_2:\mathfrak{Q}_1\cap\cdots\cap\mathfrak{Q}'_s:\mathfrak{Q}_1\ (\text{見习題 62 第 5 題})\\&=\mathfrak{Q}'_1\cap\mathfrak{Q}'_2\cap\cdots\cap\mathfrak{Q}'_s=\mathfrak{B}.\end{aligned}$$

如果 $j>1$，同理得 $\mathfrak{Q}_j:\mathfrak{Q}_1=\mathfrak{Q}_j$. 于是，

$$\begin{aligned}\mathfrak{B}=\mathfrak{B}:\mathfrak{Q}_1&=(\mathfrak{Q}_1\cap\mathfrak{Q}_2\cap\cdots\cap\mathfrak{Q}_r):\mathfrak{Q}_1\\&=\mathfrak{Q}_2\cap\mathfrak{Q}_3\cap\cdots\cap\mathfrak{Q}_r;\end{aligned}$$

这与 $\mathfrak{B}=\mathfrak{Q}_1\cap\mathfrak{Q}_2\cap\cdots\cap\mathfrak{Q}_r$ 是无贅交分解的假設矛盾.

今設 $\mathfrak{P}_1=\mathfrak{P}'_1$，則 $\mathfrak{Q}_1\cap\mathfrak{Q}'_1$ 是准素理想，以 $\mathfrak{P}_1$ 为相伴素理想. 故由上面所用的論証知，$j>1$ 时 $\mathfrak{Q}_j:(\mathfrak{Q}_1\cap\mathfrak{Q}'_1)=\mathfrak{Q}_j$，而 $i>1$ 时 $\mathfrak{Q}'_i:(\mathfrak{Q}_1\cap\mathfrak{Q}'_1)=\mathfrak{Q}'_i$. 于是，

$$\begin{aligned}\mathfrak{B}:(\mathfrak{Q}_1\cap\mathfrak{Q}'_1)&=\mathfrak{Q}_2\cap\mathfrak{Q}_3\cap\cdots\cap\mathfrak{Q}_r\\&=\mathfrak{Q}'_2\cap\mathfrak{Q}'_3\cap\cdots\cap\mathfrak{Q}'_s,\end{aligned}$$

并且这是 $\mathfrak{B}:(\mathfrak{Q}_1\cap\mathfrak{Q}'_1)$ 的两种无贅交分解，适合定理里各个条件的. 故我們可用归納法以得出素理想 $\mathfrak{P}_2,\mathfrak{P}_3,\cdots,\mathfrak{P}_r$ 的集合与 $\mathfrak{P}'_2,\mathfrak{P}'_3$，

$\cdots, \mathfrak{P}'_r$的集合相重合的結論．这就完成了定理的証明．

素理想$\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_r$的唯一性既經建立，所以就把它們叫做理想 $\mathfrak{B}$ 的**相伴素理想**．如果 $\mathfrak{B} = \mathfrak{Q}''_1 \cap \mathfrak{Q}''_2 \cap \cdots \cap \mathfrak{Q}''_t$ 是 $\mathfrak{B}$ 分解为准素理想的任意无贅分解，則可把有相同的相伴素理想的各項合併，而得定理所考究的那种形状的一个分解．故准素理想 $\mathfrak{Q}''_1, \mathfrak{Q}''_2, \cdots, \mathfrak{Q}''_t$ 的各个不同相伴素理想就是 $\mathfrak{B}$ 的相伴素理想．

唯一性定理的一个直接推論是：$\mathfrak{B}$ 是准素理想必須而且只須它仅有一个相伴素理想．換句話說：如果一个理想是准素理想的无贅交，而这些准素理想全体沒有相同的相伴素理想，則这个理想不是准素理想．

在討論另一个唯一性定理之前，我們証明下面重要的定理．

定理 6. 如果 $\mathfrak{B}$ 及 $\mathfrak{C}$ 是諾德环的理想，則 $\mathfrak{B}:\mathfrak{C} = \mathfrak{B}$ 必須而且只須 $\mathfrak{C}$ 不含于 $\mathfrak{B}$ 的任一个相伴素理想里．

証　令 $\mathfrak{B} = \mathfrak{Q}_1 \cap \mathfrak{Q}_2 \cap \cdots \cap \mathfrak{Q}_r$ 是 $\mathfrak{B}$ 分解为准素理想的一个无贅分解．令 $\mathfrak{P}_i = \mathfrak{R}(\mathfrak{Q}_i)$，并假定 $\mathfrak{C} \not\subseteq \mathfrak{P}_i$．則由引理 3 得 $\mathfrak{Q}_i:\mathfrak{C} = \mathfrak{Q}_i$．故

$$\begin{aligned}\mathfrak{B}:\mathfrak{C} &= (\mathfrak{Q}_1 \cap \mathfrak{Q}_2 \cap \cdots \cap \mathfrak{Q}_r):\mathfrak{C}\\ &= \mathfrak{Q}_1:\mathfrak{C} \cap \mathfrak{Q}_2:\mathfrak{C} \cap \cdots \cap \mathfrak{Q}_r:\mathfrak{C}\\ &= \mathfrak{Q}_1 \cap \mathfrak{Q}_2 \cap \cdots \cap \mathfrak{Q}_r = \mathfrak{B}.\end{aligned}$$

反过来，設对于某个 i 有 $\mathfrak{C} \subseteq \mathfrak{P}_i$；譬如說，$\mathfrak{C} \subseteq \mathfrak{P}_1$．則有一个整数 m 存在使 $\mathfrak{C}^m \subseteq \mathfrak{Q}_1$．于是，

$$\mathfrak{C}^m(\mathfrak{Q}_2 \cap \cdots \cap \mathfrak{Q}_r) \subseteq \mathfrak{C}^m \cap \mathfrak{Q}_2 \cap \cdots \cap \mathfrak{Q}_r \subseteq \mathfrak{B}.$$

令 n 是最小整数使

$$\mathfrak{C}^n(\mathfrak{Q}_2 \cap \cdots \cap \mathfrak{Q}_r) \subseteq \mathfrak{B}. \tag{12}$$

因为 $\mathfrak{B} = \mathfrak{Q}_1 \cap \cdots \cap \mathfrak{Q}_r$ 是无贅交，故 $n \geqslant 1$．于是，$\mathfrak{C}^{n-1}(\mathfrak{Q}_2 \cap \cdots \cap \mathfrak{Q}_r) \not\subseteq \mathfrak{B}$[1]．另一方面，由(12)得 $\mathfrak{C}^{n-1}(\mathfrak{Q}_2 \cap \cdots \cap \mathfrak{Q}_r) \subseteq \mathfrak{B}:\mathfrak{C}$．故 $\mathfrak{B}:\mathfrak{C} \supset \mathfrak{B}$．

今設 $\mathfrak{Q}'_1 \cap \mathfrak{Q}'_2 \cap \cdots \cap \mathfrak{Q}'_s$ 是 $\mathfrak{C}$ 分解为无贅交的一个分解，它的

---

1) 我們規定 $\mathfrak{C}^0(\mathfrak{Q}_2 \cap \cdots \cap \mathfrak{Q}_r) = \mathfrak{Q}_2 \cap \cdots \cap \mathfrak{Q}_r$．——著者注．

相伴素理想是 $\mathfrak{P}'_1, \mathfrak{P}'_2, \cdots, \mathfrak{P}'_s$. 如果 $\mathfrak{C} \subseteq \mathfrak{P}_1$, 則 $\mathfrak{Q}'_1\mathfrak{Q}'_2\cdots\mathfrak{Q}'_s \subseteq \mathfrak{P}_1$. 于是,有一个 $\mathfrak{Q}'_j$ 含于 $\mathfrak{P}_1$ 里,从而有一个 $\mathfrak{P}'_j$ 含于 $\mathfrak{P}_1$里. 反过来,如果 $\mathfrak{P}'_j \subseteq \mathfrak{P}_1$, 显然 $\mathfrak{C} \subseteq \mathfrak{P}'_j \subseteq \mathfrak{P}_1$. 应用这个說明,可把上面的判别准则改述如次:

定理 6′. 如果 $\mathfrak{B}$ 及 $\mathfrak{C}$ 是諾德环的理想,則 $\mathfrak{B}:\mathfrak{C} = \mathfrak{B}$ 必須而且只須 $\mathfrak{C}$ 的相伴素理想沒有一个含于 $\mathfrak{B}$ 的任一个相伴素理想里.

我們将应用这个判别准則导出第二唯一性定理; 这定理牽涉到理想 $\mathfrak{B}$ 的孤立部分. 如果 $\mathfrak{B}$ 由无贅交 $\mathfrak{Q}_1 \cap \mathfrak{Q}_2 \cap \cdots \cap \mathfrak{Q}_r$ 表出,这里$\mathfrak{Q}_i$是准素理想,并且它們有不同的相伴素理想$\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_r$. 如果分解里某个 $\mathfrak{Q}$ 的相伴素理想不含有 $\mathfrak{B}$ 的其他相伴素理想,則这个 $\mathfrak{Q}$ 叫做 $\mathfrak{B}$ 的一个**孤立准素理想**. 更一般的, 如果 $\mathfrak{Q}_{i_1} \cap \mathfrak{Q}_{i_2} \cap \cdots \cap \mathfrak{Q}_{i_n}$ 里各項的相伴素理想 $\mathfrak{P}_{i_j} (j = 1, 2, \cdots, n)$ 沒有一个含有这些項以外任一項的相伴素理想, 則 $\mathfrak{Q}_{i_1} \cap \mathfrak{Q}_{i_2} \cap \cdots \cap \mathfrak{Q}_{i_n}$ 叫做 $\mathfrak{B}$ 的一个**孤立部分**. 今述

第二唯一性定理 令 $\mathfrak{B} = \mathfrak{Q}_1 \cap \mathfrak{Q}_2 \cap \cdots \cap \mathfrak{Q}_r = \mathfrak{Q}'_1 \cap \mathfrak{Q}'_2 \cap \cdots \cap \mathfrak{Q}'_r$ 是$\mathfrak{B}$的两个分解,适合第一唯一性定理的各个条件. 令 $\mathfrak{C} = \mathfrak{Q}_{i_1} \cap \mathfrak{Q}_{i_2} \cap \cdots \cap \mathfrak{Q}_{i_k}$ 是第一种分解里一个孤立部分, 而 $\mathfrak{C}'$ 是第二种分解里孤立部分,它与$\mathfrak{C}$有相同的相伴素理想集合,則$\mathfrak{C} = \mathfrak{C}'$.

証 命 $\mathfrak{B} = \mathfrak{C} \cap \mathfrak{D} = \mathfrak{C}' \cap \mathfrak{D}'$, 这里 $\mathfrak{D}$ 及 $\mathfrak{D}'$ 分别是 $\mathfrak{Q}_i$ 及 $\mathfrak{Q}'_i$ 的交,它們是不含有 $\mathfrak{C}$ 及 $\mathfrak{C}'$ 的. 則 $\mathfrak{D} \cap \mathfrak{D}'$ 的相伴素理想不含于 $\mathfrak{C}$ 的任何相伴素理想里. 故 $\mathfrak{C}:(\mathfrak{D} \cap \mathfrak{D}') = \mathfrak{C}$. 同理,得 $\mathfrak{C}':(\mathfrak{D} \cap \mathfrak{D}') = \mathfrak{C}'$. 于是,

$$\mathfrak{B}:(\mathfrak{D} \cap \mathfrak{D}') = (\mathfrak{C}:(\mathfrak{D} \cap \mathfrak{D}')) \cap (\mathfrak{D}:(\mathfrak{D} \cap \mathfrak{D}')) = \mathfrak{C},$$

并且

$$\mathfrak{B}:(\mathfrak{D} \cap \mathfrak{D}') = (\mathfrak{C}':(\mathfrak{D} \cap \mathfrak{D}')) \cap (\mathfrak{D}':(\mathfrak{D} \cap \mathfrak{D}')) = \mathfrak{C}'.$$

故 $\mathfrak{C} = \mathfrak{C}'$.

注記. 另一个唯一性定理,即关于一个理想的不可約部分的个数的唯一性定理将于下一章 §5 里証明.

习 题 67

1. 如果 $\mathfrak{B}$ 的所有相伴素理想是极大的,求証: $\mathfrak{B}$ 分解为带有不同相伴素理想的

准素理想的无赘交只有一种分解法.

2. 求証:諾德环里理想的根集是相伴素理想的交.

3. 求証:根集是一个素理想必須而且只須給定的理想只有一个孤立准素理想.

4. 如果$\mathfrak{B}$是一个理想,则$\bigcap_i \mathfrak{B}^i (i = 1,2,3\cdots)$叫做$\mathfrak{B}$的$\omega$-冪,記作$\mathfrak{B}^{\omega}$. 令$\mathfrak{B}$是諾德环里一个理想,并令$\mathfrak{B}^{\omega}\mathfrak{B} = \mathfrak{Q}_1 \cap \mathfrak{Q}_2 \cap \cdots \cap \mathfrak{Q}_n$是准素理想的无贅交. 求証:$\mathfrak{Q}_j \supseteq \mathfrak{B}^{\omega} (j = 1,2,\cdots,n)$. 由此求証: $\mathfrak{B}^{\omega}\mathfrak{B} = \mathfrak{B}^{\omega}$.

9. 整性相关 下面要說的概念是代数整数上古典概念的拓广. 如果一个复数是整系数的簡型多項式(亦即系数是整数并且x的最高冪的系数为1的多項式)的一个根,这种复数叫做代数整数. 今令$\mathfrak{A}$是任一个带恆等元素的交換环,并令$\mathfrak{g}$是$\mathfrak{A}$的子环含有1. 如果元素$a \in \mathfrak{A}$适合簡型方程$f(x) = 0$,这里$f(x) \in \mathfrak{g}[x]$,則說a对于$\mathfrak{g}$整性相关,或說a是一个$\mathfrak{g}$-整数. 如果

$$f(x)=x^n-\gamma_{n-1}x^{n-1}-\cdots-\gamma_0,\quad \gamma_c\in\mathfrak{g},$$

則

$$a^n = \gamma_0 + \gamma_1 a + \cdots + \gamma_{n-1}a^{n-1}. \tag{13}$$

由此可見,a的所有冪可写成$1, a, \cdots, a^{n-1}$的綫性組合,它的系数属于$\mathfrak{g}$.

显然$\mathfrak{A}$可看作一个$\mathfrak{g}$-模的;这模的羣是$\mathfrak{A}, +$,而$\mathfrak{g}$的元素按环的乘法来乘. 于是,前面的結果是:如果a是一个$\mathfrak{g}$-整数,并且(13)成立,則a的所有冪都含于有限生成的$\mathfrak{g}$-模$(1, a, \cdots, a^{n-1})$里. 反过来,也显然成立的;这因为,如果$a^n \in (1, a, \cdots, a^{n-1})$,則有(13)形状的一个关系.

本节此后假定$\mathfrak{g}$是諾德环,并且将考究$\mathfrak{g}$-整元素的全体. 所用的主要工具是下面的模判定准則:

定理 7. 如果$\mathfrak{g}$是諾德环,則$\mathfrak{A}$里元素a是一个$\mathfrak{g}$-整数必須而且只須$\mathfrak{A}$有一个有限生成的子模存在,含有a的所有冪.

証 由上面論証知这个条件是必要的. 今証充分性. 令$\mathfrak{N}$是一个有限生成的$\mathfrak{g}$-模,含有a的所有冪. 因为$\mathfrak{g}$是諾德环,故$\mathfrak{N}$适合关于子模的升鏈条件. 于是,有一个整数n存在,使升鏈

$$(1)\subseteq(1,a)\subseteq(1,a,a^2)\subseteq\cdots$$

里有$(1, a, \cdots, a^{n-1}) = (1, a, \cdots, a^n)$. 由此推知,$a^n \in (1, a, \cdots,$

a^{n-1}). 故得(13)形状的一个关系.

今用这个判别准则来证下面的定理.

定理8. $\mathfrak{A}$ 里 $\mathfrak{g}$-整數的全体 $\mathfrak{G}$ 是 $\mathfrak{A}$ 的一个子环,含有 $\mathfrak{g}$.

証 $\mathfrak{g}$ 的任一个元素 γ 适合方程 $x-\gamma=0$, 故它属于 $\mathfrak{G}$. 次令 a 及 b 都属于 $\mathfrak{G}$,并令$(u_1,u_2,\cdots,u_s)$及$(v_1,v_2,\cdots,v_t)$是 $\mathfrak{A}$ 的两个 $\mathfrak{g}$-模,分别含有 a 及 b 的所有冪. 則(u_i)的任一个元素与(v_j)的任一个元素的积属于子模

$$\mathfrak{P}=(u_1v_1,\cdots,u_1v_t;u_2v_1,\cdots,u_2v_t;\cdots;\cdots,u_sv_t).$$

所以形状如 a^kb^l 的任一个单项式属于 $\mathfrak{P}$. 于是, $a\pm b$ 及 ab 的所有冪都属于$\mathfrak{P}$. 故 $a+b$ 及 ab 属于 $\mathfrak{G}$, 而 $\mathfrak{G}$ 是 $\mathfrak{A}$ 的一个子环.

如果 $\mathfrak{G}=\mathfrak{g}$, 亦即如果 $\mathfrak{A}$ 里对于 $\mathfrak{g}$ 整性相关的每个元素属于 $\mathfrak{g}$,則說 $\mathfrak{g}$ 在 $\mathfrak{A}$ 里整性封閉. 今証

定理 9. $\mathfrak{g}$-整元素的环 $\mathfrak{G}$ 在 $\mathfrak{A}$ 里整性封閉.

証 令 a 是一个 $\mathfrak{G}$-整数,并令

$$a^n=g_0+g_1a+\cdots+g_{n-1}a^{n-1},g_i\in\mathfrak{G}.$$

我們可用这个关系証明: a 的每个冪可由 $1,a,\cdots,a^{n-1}$ 綫性組合表出, 而系数是含 g 的单項式的和. 簡单扩张前定理里証明的論点,可証: $\mathfrak{A}$ 里存在一个有限生成的 $\mathfrak{g}$-子模 $(w_1,w_2,\cdots,w_l)$,包含 g 的所有单項式. 于是, a 的每个冪显然含于

$$(w_1,\cdots,w_l;w_1a,\cdots,w_la;\cdots;\cdots,w_la^{m-1}).$$

故 $a\in\mathfrak{G}$,这就是我們所要証明的.

如果 $\mathfrak{A}=\mathfrak{F}$ 是一个域,而 $\mathfrak{g}=\mathfrak{F}_0$ 是一个子域,則 $\mathfrak{F}$ 的一个元素是 $\mathfrak{F}_0$-整元素必須而且只須它是 $\mathfrak{F}_0$ 上代数元素(§7). 故在这情形下, 定理 8 就变做: $\mathfrak{F}$ 里 $\mathfrak{F}_0$ 上代数元素的集合 $\mathfrak{G}$ 是 $\mathfrak{F}$ 里含有 $\mathfrak{F}_0$ 的一个子环. 我們还知道,如果 a 是代数元素, 則 $\mathfrak{F}_0[a]$是一个子域. 所以,如果 $a\neq 0$, 則 $a^{-1}\in\mathfrak{F}_0[a]\subseteq\mathfrak{G}$. 故 $\mathfrak{G}$ 是一个域. 如果把定理 9 也結合进去,則得关于域的下面重要的定理.

定理10. 令 $\mathfrak{F}$ 是一个域, 而 $\mathfrak{F}_0$ 是一个子域, 則 $\mathfrak{F}$ 里 $\mathfrak{F}_0$ 上代數元素的集合 $\mathfrak{G}$ 構成 $\mathfrak{F}$ 的一个子域,含有 $\mathfrak{F}_0$. $\mathfrak{F}$ 里任一个 $\mathfrak{G}$ 上的代數元素必屬于 $\mathfrak{G}$.

今令 $\mathfrak{F}$ 是任一个域，令 $\mathfrak{g}$ 是 $\mathfrak{F}$ 的任一个子环含有 1，并令 $\mathfrak{F}_0$ 表 $\mathfrak{F}$ 里由 $\mathfrak{g}$ 生成的子域．如果元素 $a \in \mathfrak{F}$ 是 $\mathfrak{g}$-整数，则一定是 $\mathfrak{F}_0$ 上代数元素．故它的极小多项式 $\mu(x)$ 是系数 $\in \mathfrak{F}_0$ 的簡型多項式．今将証明：如果 $\mathfrak{g}$ 是高斯环，则 $\mu(x) \in \mathfrak{g}[x]$．要証这結果，令 $f(x)$ 是系数 $\in \mathfrak{F}_0$ 的簡型多項式，并且 $f(a) = 0$，則 $\mu(x) | f(x)$．但 $f(x)$ 在 $\mathfrak{g}[x]$ 里的不可約因子中有一个是 $\mu(x)$ 在 $\mathfrak{F}_0[x]$ 里的相伴多項式．令这个因子为 $\mu^*(x)$，則 $\mu^*(x) = \beta\mu(x)$，这里 $\beta \in \mathfrak{F}_0$．因为 $f(x)$ 是簡型多項式，并且 $\mu^*(x) | f(x)$，故可假定 $\mu^*(x)$ 也是簡型的．于是，由 $\mu^*(x) = \beta\mu(x)$ 得 $\beta = 1$；从而 $\mu(x) = \mu^*(x) \in \mathfrak{g}[x]$．这証明了下面的定理．

定理11. 令 $\mathfrak{g}$ 是域 $\mathfrak{F}$ 里一个高斯子环，并令 $\mathfrak{F}_0$ 是 $\mathfrak{F}$ 的子域由 $\mathfrak{g}$ 生成的，則 $\mathfrak{F}$ 里一个元素 a 对于 $\mathfrak{g}$ 整性相关必須而且只須它是 $\mathfrak{F}_0$ 上代数元素，并且它的 $\mathfrak{F}_0$ 上極小多項式的系數屬于 $\mathfrak{g}$．

如果 $\mathfrak{F}$ 的每个元素是 $\mathfrak{F}_0$ 上代数元素，則这个判別准則是特別有用的．这因为，此时它肯定了：$\mathfrak{F}$ 的元素是 $\mathfrak{g}$-整数必須而且只須它的极小多項式 $\in \mathfrak{g}[x]$．又因为 $\mathfrak{F}_0$ 的元素是 $\mathfrak{F}_0$ 上代数元素，并且有 $x - \gamma$ 形状的极小多項式，所以 $\mathfrak{F}_0$ 的元素能够成 $\mathfrak{g}$ 上整元素的只有 $\mathfrak{g}$ 里元素．故 $\mathfrak{g}$ 在 $\mathfrak{F}_0$ 里整性封閉．如果一个整区在它的分式域里成整性封閉，則它叫做**整性封閉整区**．于是，我們所得結果可述成下面的系．

系 任一个高斯整区是整性封閉的．

10. 二次域的整数 代数数論涉及形状如 $R_0(\theta)$ 的域的算术性質，这里 R_0 是有理数域，而 θ 是一个代数元素．这个理論研究的原始对象是 $R_0(\theta)$ 里能够成 I-整数（或簡称做 $R_0(\theta)$ **的整数**）的元素的环 $\mathfrak{G}$．本节借决定二次扩张 $R_0(\theta)$ 的整数环来簡单介紹代数数論．

令 m 是一个（普通）整数，它不含平方因子．則多項式 $x^2 - m$ 在 $I[x]$ 里是不可約的．因为 I 是高斯环，故 $x^2 - m$ 在 $R_0[x]$ 里是不可約的．于是，可作一个扩张域 $R_0(\theta)$，这里 $\theta^2 = m$．这种域叫做有理数域的一个**二次扩张**．

$R_0(\theta)$的任一个元素必有而且只有一种方法写成 $u = \alpha + \beta\theta$ 形状，这里 α 及 $\beta \in R_0$. 如果 $u = \alpha + \beta\theta$, 則元素 $\bar{u} = \alpha - \beta\theta$ 叫做 u (在 $R_0(\theta)$里)的**共軛元素**. 我們易知，映照 $u \to \bar{u}$ 是 $R_0(\theta)$的一个自同构. 显然，如果 $u \notin R_0$, 則 $\bar{u} \neq u$. 令

$$T(u) = u + \bar{u} = 2\alpha,\ N(u) = u\bar{u} = \alpha^2 - \beta^2 m,$$

則 $T(u)$ 及 $N(u)$ 都 $\in R_0$. 于是，多项式

$$f(x, u) = (x - u)(x - \bar{u}) = x^2 - T(u)x + N(u)$$

的系数是有理数. 显然，u 是 $f(x, u)$的一个根. 故$R_0(\theta)$的每个元素是 R_0 上代数元素.

如果 $u \in R_0$, 則 u 对于 I 整性相关必須而且只須 $u \in I$. 如果 $u \notin R_0$, 則 u 关于 R_0 的极小多項式的次数 > 1. 故它是多項式 $f(x, u)$. 于是，u 是 $R_0(\theta)$的一个整数必須而且只須 $T(u)$及 $N(u)$ 的系数是整数. 故得条件

(14) $$2\alpha \in I,\ \alpha^2 - \beta^2 m \in I.$$

由第一个条件可推得 $\alpha \in I$, 或 α 是奇整数的二分之一，即 $\alpha = (2n + 1)/2$. 如果 $\alpha \in I$, 則由第二个条件得 $\beta^2 m \in I$. 因为 m 沒有平方因子，故知 $\beta \in I$; 否則 $\beta = b_1 b_2^{-1}$, 这里 b_1 及 $b_2 \in I$, 并且有一个素数 p 能除尽 b_2. 但不能除尽 b_1. 于是，

$$b_1^2 m = (\beta^2 m) b_2^2 \equiv 0 (\mathrm{mod}\, p^2).$$

因为 $p \nmid b_1$, 故必 $p^2 | m$, 这就与假設矛盾了.

次設 $\alpha = (2n + 1)/2$, 这里 $n \in I$. 此时，由条件 $N \equiv \alpha^2 - \beta^2 m \in I$ 得

$$\beta^2 m = \alpha^2 - N = (4n^2 + 4n - 4N + 1)/4.$$

故

(15) $$\beta^2 m = (4r + 1)/4,\ r \in I.$$

令 $\beta = b_1 b_2^{-1}$, 这里 b_1 及 b_2 是使 $(b_1, b_2) = 1$ 的整数. 以 $4b_2^2$ 乘 (15), 得

$$4b_1^2 m = (4r + 1) b_2^2.$$

因为 m 不含平方因子，并且 $(b_1, b_2) = 1$, 故由这个关系可推得 $b_2^2 = 4$, 从而 $b_2 = \pm 2$. 于是，b_1 是奇数，而 β 是奇整数的二分之

一.

今令 $\beta = (2q + 1)/2, \alpha = (2n + 1)/2$. 因为

$$N = \alpha^2 - \beta^2 m = [4n^2 + 4n + 1 - (4q^2 + 4q + 1)m]/4$$

是一个整数,故得同余式

$$4n^2 + 4n + 1 - (4q^2 + 4q + 1)m \equiv 0 \pmod{4}.$$

它約簡为 $1 - m \equiv 0 \pmod{4}$, 亦即 $m \equiv 1 \pmod{4}$. 故知,除非 m 的形状是 $4k + 1$ 外, $R_0(\theta)(\theta^2 = m)$的整数必須是 $\alpha + \beta\theta$ 的形状,这里 α 及 β 是普通整数. 如果 $m \equiv 1 \pmod{4}$, 則还可能有另一种如 $\alpha + \beta\theta$ 形状的整数,其中 α 及 β 都是奇整数的二分之一.

反过来,如果 α 及 $\beta \in I$,則(13)成立,而 $\alpha + \beta\theta$ 是一个二次整数. 再則,如果 $m \equiv 1 \pmod{4}$, 并且 α 及 β 是奇整数的二分之一,則 $\alpha + \beta\theta$ 是一个二次整数. 我們的結論可綜述如次:

定理12. 令 m 是一个不含平方因子的整数. 如果 $m \equiv 2$ 或 $3 \pmod{4}$,則 $R_0(\theta)$ 是環 $\mathfrak{G}$ 里形状如 $\alpha + \beta\theta$ 的数的集合,这里 α 及 $\beta \in I$;如果 $m \equiv 1 \pmod{4}$, 則 $\mathfrak{G}$ 是形状如 $\alpha + \beta\theta$ 的数的集合,这里 α 及 β 都 $\in I$,或者都是奇整数的二分之一.

习 題 68

1. 如果 $m = -3$. 求証: $\mathfrak{G}$ 是歐几里得整区.
2. 求証: m 只有五个負值,即 $m = -1, -2, -3, -7, -11$, 使 $\mathfrak{G}$ 关于函数 $\delta(\alpha) = |N(\alpha)|$ 成歐几里得整区. [1]

---

1) 例如,参看哈地(Hardy)及烏来特(Wright)著的数論(The Theory of Numbers, Oxford, 1938 年版), 第 213 頁. m 的正值中能使这結果成立的是: $m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73, 97$, 这是晚近才决定出来的. 参看謝兰得(H. Chatland)的論文:关于二次域里的欧几里得算法(On the Euclidean algorithm in quadratic number fields), 載在美国数学会紀事 (Bull. Amer. Math. Soc.),卷 55(1949),第 948—953 頁. 关于欧几里得除法方法的存在毋須利用函数 $\delta(\alpha) = |N(\alpha)|$ 的問題,曾在莫兹京 (T. Motzkin) 的論文:"欧克里得算法 (The Euclidean algorithm)" 中討論, 这篇論文載在美国数学会紀事, 卷 55(1949),第1142—1146頁. ——著者注.

第 七 章

格

在羣論及环論的若干重要討論里，人們最初宁愿涉到这些代数系的一些特殊子集合（不变子羣，理想），而不只限元素自身. 特别在約当-霍尔德-叔萊尔的理論是如此的. 它的論点牽涉到由 M-子羣构成的代数系，及这些代数系里交与生成的羣两种合成. 同样，环論的一些部分牽涉到由（左、右、双侧）理想构成的代数系，及这些代数系里交与和两种合成. 所以就导致一种抽象代数系叫做格；它包括这两个代数系作为特例. 格的概念，首由狄得京（Dedekind）定义，但直到近来（1930 年前后）才受到人們的注意. 除了代数上应用以外，在几何基础及其他部門上还发現許多应用. 应該指出，布尔（Boole）在狄得京以前就曾經引出一类特殊的格，叫做布尔代数.

本章将簡短叙述格論里可应用于羣論及环論的那些部分. 所用論証常是前面遇到的論証的重复，在这样情形下就不作詳尽的闡述.

1. 半序集合

定义 1. 半序集合是由一个集合 S 及一个关系 $\geqslant$（"大或等于"或"含有"）构成的一个代数系，适合下面的公理：

P_1. 要 $a \geqslant b$ 及 $b \geqslant a$ 成立，必須而且只須 $a = b$.

P_2. 如果 $a \geqslant b$ 及 $b \geqslant c$，則 $a \geqslant c$.

如果 a 及 b 是 S 的任意元素，則或有 $a \geqslant b$，或沒有这个关系；在后一种情形，就記作 $a \not\geqslant b$. 又或 $a \geqslant b$，但 $a \neq b$. 則記作 $a > b$. 我們还同意把 $a \geqslant b$ 及 $a > b$ 写做 $b \leqslant a$ 及 $b < a$.

例. （1）整数的集合 I，正整数的集合 P 及实数的集合 R 关于通常的 $\geqslant$ 关系都

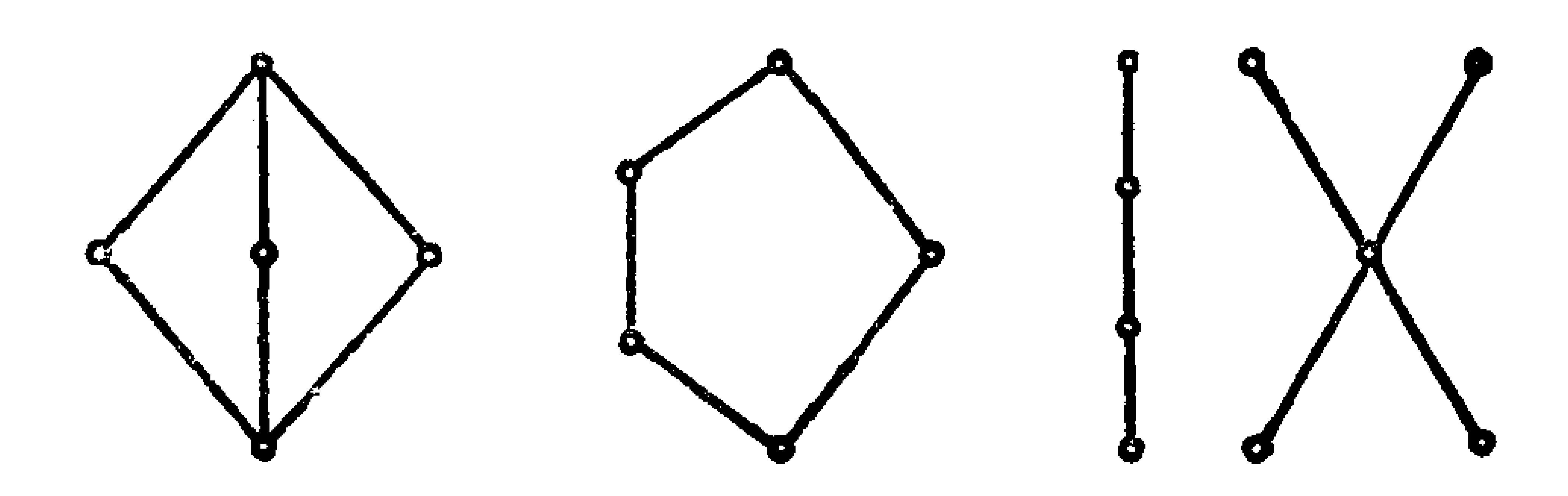
是半序集合. (2) 正整数的集合 P, 关系 $\geqslant$ 的意义规定为:如果 $a|b$, 则 $a \geqslant b$. 这样定义的关系显然适合 P_1 及 P_2. (3) 一个任意集合 S 的子集合所构成的集合 $\mathfrak{P}$, 規定 $A \geqslant B$ 的意义为: B 是 A 的一个子集合. (4) 羣 $\mathfrak{G}$ 的子羣所构成的集合 $\mathfrak{L}$, $\mathfrak{H}_1 \geqslant \mathfrak{H}_2$ 的意义与 (3) 的規定相同.

在例 (2), (3) 或 (4) 的任一个里都存在有不能比較的元素 a 及 b, 亦即 $a \geqslant b$ 或 $b \geqslant a$ 都不成立. 如果一个半序集合 S 里, 每两个元素都是可比較的 ($a \geqslant b$ 或 $b \geqslant a$), 则說: S 是**綫性序集合**, 或 S 是一个**鏈**. (1) 里所有的例都属于这个类型.

在一个有限半序集合里, 可以复盖关系表示关系 $>$. 如果 $a_1 > a_2$, 并且沒有 u 存在使 $a_1 > u > a_2$, 则說 a_1 是 a_2 的一个**复盖**. 在一个有限半序集合里, 如果 $a > b$, 显然可求得一个鏈

$$a = a_1 > a_2 > \cdots > a_n = b,$$

使每个 a_i 复盖 a_{i+1}. 反过来, 这样鏈的存在可推得 $a > b$. 由这个說明使我們能够以图解来表示任一个有限半序集合. 我們可以小圓(或点)表示 S 的元素; 如果 a_1 是 a_2 的复盖, 则置表 a_1 的圓于表 a_2 的圓的上方, 并联以直綫, 就得到图解. 故 $a > b$ 必須而且只須由 a 到 b 有一个下降的折綫联絡着. 这种图解的一些例子如次:



半序集合的图解的概念显然給我們另一种作出这样集合的例子的方法.

习　题 69

1. 求証: 由阶数为素数冪的一个循环羣的子羣构成的半序集合是一个鏈.
2. 令 S 是在区間 $0 \leqslant x \leqslant 1$ 上連續的所有函数的集合, 并定义 $f \geqslant g$, 必須而且只須对于閉区間內所有 x, $f(x) \geqslant g(x)$. 求証: 关系 $\geqslant$ 是 S 的一个半序关系.
3. 求下列半序集合的图解: 由含有三个元素的集合的子集合构成的集合; 6 阶循环羣的子羣构成的集合; S_3 的子羣构成的集合.

2. 格 設 S 是半序集合，A 是 S 的子集合，如果 S 里有一个元素 u 对于 A 里每个元素 a，有 $u \geqslant a$，則說 u 是 A 的一个上界．如果 u 是 A 的一个上界，并且 A 的任一个上界 v 适合 $u \leqslant v$，則 u 叫做 A 的一个最小上界，簡記作 l. u. b. 我們易知，如果有一个最小上界存在，則它是唯一的．关于下界及最大下界(簡記作 g. l. b.)也有类似的定义及說明．这些概念是下面定义的基础．

定义 2. 如果一个半序集合里任意两个元素有一个最小上界及一个最大下界，这个集合叫做格(結构)．

我們以 $a \cup b$ 表 a 与 b 的 l. u. b. ("a 合并 b")，并以 $a \cap b$ 表 g. l. b. ("a 交 b")．如果 a, b, c 是格 L 里任意三个元素，則 $(a \cup b) \cup c \geqslant a, b, c$．不但如此，如果 v 是 $\geqslant a, b, c$ 的任一个元素，則 $v \geqslant (a \cup b), c$．于是，$v \geqslant (a \cup b) \cup c$．故 $(a \cup b) \cup c$ 是 a, b 及 c 的 l. u. b. 由簡单归納的論証可知，S 的任一个有限子集合必有一个 l. u. b.; 同理，任一个有限子集合必有一个 g. l. b.．如果这个集合由 $a_1, a_2, \cdots, a_n$ 构成，則 l. u. b. 及 g. l. b. 分别記为

$$a_1 \cup a_2 \cup \cdots \cup a_n \quad 及 \quad a_1 \cap a_2 \cap \cdots \cap a_n.$$

如果任一个(有限或无限)子集合 $A = \{a_\alpha\}$ 有一个 l. u. b.．$\cup a_\alpha$ 及一个 g. l. b. $\cap a_\alpha$，則格 L 叫做完全格．

在 §1 里，例 (1)—(4) 所列的半序集合都是格．在例 (3)提到的，一个集合的子集合所构成的集合里，$A \cup B$ 及 $A \cap B$ 具有通常集合論上的和及集合交的意义．在羣 $\mathfrak{G}$ 的子羣构成的半序集合里，$\mathfrak{H}_1 \cup \mathfrak{H}_2$ 是由 $\mathfrak{H}_1$ 及 $\mathfrak{H}_2$ 生成的羣 $[\mathfrak{H}_1, \mathfrak{H}_2]$，而 $\mathfrak{H}_1 \cap \mathfrak{H}_2$ 是通常的交．§1 所列出的各图解中，除最后一个外，都表示格．任一个集合的子集合构成的格及任一个羣的子羣构成的格都是完全格．有理数构成的格(用通常的 $\geqslant$) 不是完全格．

在一个格里，二元合成 $\cup$ 及 $\cap$ 的代数基本性质是值得枚列的．要这样做，我們将引出格的另一个更代数化的定义．

首先要說的是：两个元素的 l. u. b. 及 g. l. b. 是元素的对称函数，亦即 $a \cup b = b \cup a$ 及 $a \cap b = b \cap a$．我們还知道，$(a \cup b) \cup c$ 是 a, b, c 的 l. u. b.．因为 l. u. b. 是唯一的，故

$$(a\cup b)\cup c=(b\cup c)\cup a=a\cup(b\cup c).$$

同理，得

$$(a\cap b)\cap c=a\cap(b\cap c).$$

显然

$$a\cup a=a,\quad a\cap a=a.$$

因为 $a\cup b\geqslant a$，故 $(a\cup b)\cap a=a$. 同理，得 $(a\cap b)\cup a=a$.

反过来，設 L 是任一个集合，在这个集合里定义有两个二元合成 $\cup$ 及 $\cap$，适合

L_1. $a\cup b=b\cup a,\quad a\cap b=b\cap a$.

L_2. $(a\cup b)\cup c=a\cup(b\cup c),\quad (a\cap b)\cap c=a\cap(b\cap c)$.

L_3. $a\cup a=a,\quad a\cap a=a$.

L_4. $(a\cup b)\cap a=a,\quad (a\cap b)\cup a=a$.

我們将証明，在給 $\geqslant$ 以适宜定义下，L 关于 $\geqslant$ 是一个格，并且 $\cup$ 及 $\cap$ 是这个格里的 l. u. b. 及 g. l. b..

在进行証明前，可注意的是：我們对于两个合成 $\cup$ 及 $\cap$ 作了相同的假設. 故关于 $\cup$ 及 $\cap$ 存在有重要的对偶原理，就是說，如果 S 是由上面各公理演繹出的一个命題，則于 S 里把 $\cup$ 与 $\cap$ 互相替换，得出的对偶命題一定也可由公理演繹出.

其次要說的是：如果 a 及 b 是适合 L_1—L_4 的代数系里元素，則条件 $a\cup b=a$ 与 $a\cap b=b$ 等价. 这因为，如果 $a\cup b=a$ 成立，則 $a\cap b=(a\cup b)\cap b=b$；而由对偶方面，也可从 $a\cap b=b$ 推得 $a\cup b=a$. 今于 L 里定义关系 $\geqslant$ 如次：$a\geqslant b$ 表明 $a\cup b=a$ 或 $a\cap b=b$. 要找一个命題的对偶命題显然是以 $b\geqslant a$ 替代 $a\geqslant b$.

今来証明半序集合的基本法則 P_1—P_2 对于上面定义的关系能够成立. 設 $a\geqslant b$，并且 $b\geqslant a$，則 $a\cup b=a$，并且 $b\cup a=b$. 故由交换律得 $a=b$. 又由 L_3 知，$a\cup a=a$，故 $a\geqslant a$. 这証明了 P_1. 次設 $a\geqslant b$，并且 $b\geqslant c$，則有 $a\cup b=a$ 及 $b\cup c=b$. 于是，

$$a\cup c=(a\cup b)\cup c=a\cup(b\cup c)=a\cup b=a,$$

而 $a\geqslant c$. 故 P_2 也成立.

因为 $(a\cup b)\cap a=a$，故 $a\cup b\geqslant a$. 同理得 $a\cup b\geqslant b$. 今命

c是适合 $c \geqslant a$ 及 $c \geqslant b$ 的任一个元素，则 $a \cup c = c$，并且 $b \cup c = c$。于是，

$$(a \cup b) \cup c = a \cup (b \cup c) = a \cup c = c,$$

而 $c \geqslant a \cup b$. 这証明了 $a \cup b$ 是 a 与 b 的一个 l. u. b.. 由对偶性知，$a \cap b$是 a 与 b 的一个 g. l. b.. 綜上所論，可見适合 L_1—L_4 的代数系是格.

如果格 L 的一个子集合M对于合成 $\cup$ 及 $\cap$ 封閉，则M叫做**子格**. 显然子格关于导出的合成是一个格. 反过来，格 L 的一个子集合关于 L 里所定义的半序关系 $\geqslant$ 可以是一个格，而不是一个子格. 例如，令 $\mathfrak{G}$ 是一个羣，$\mathfrak{P}$ 是 $\mathfrak{G}$ 的子集合构成的格. $\mathfrak{L}$ 是 $\mathfrak{G}$ 的子羣构成的格. 显然，$\mathfrak{L} \subseteq \mathfrak{P}$，并且在这两个集合里，$\mathfrak{H}_1 \geqslant \mathfrak{H}_2$ 有相同的意义. 但，如果 $\mathfrak{H}_1$ 及 $\mathfrak{H}_2$ 是子羣，则 $\mathfrak{H}_1 \cup \mathfrak{H}_2$ 在 $\mathfrak{P}$ 里决定了这两个子羣的集合論上的和，一般它不是一个子羣；而在 $\mathfrak{L}$ 里，$\mathfrak{H}_1 \cup \mathfrak{H}_2$ 乃决定 $\mathfrak{G}$ 里含有 $\mathfrak{H}_1$ 及 $\mathfrak{H}_2$ 的最小子羣. 这种差别显示 $\mathfrak{L}$ 不是 $\mathfrak{P}$ 的子格.

如果 a 是格 L 的一个固定元素，则使 $x \geqslant a$ $(x \leqslant a)$ 的元素 x 的子集合显然是一个子格. 如果 $a \geqslant b$，则使 $a \geqslant x \geqslant b$ 的元素 x 的子集合是一个子格；这样的子格叫做一个(閉)**区間**(**商**)，記作 $I[a,b]$[1].

格用公理 L_1—L_4 作出的定义还可引向同态的有用定义. 如果格 L 到格 L' 的映照 $a \rightarrow a'$ 适合

$$(a \cup b)' = a' \cup b', \text{ 及 } (a \cap b)' = a' \cap b',$$

这个映照叫做**同态**. 如果这种映照是 1—1 的，则叫做**同构**. 关于同构的一个有用判别准则是下面的定理.

定理 1. 格 L 到格 L' 上的一个 1—1 映照 $a \rightarrow a'$ 是同構必須而且只須从 L 里 $a \geqslant b$ 可推得 L' 里 $a' \geqslant b'$，並且从 L' 里 $a' \geqslant b'$ 也可推得 L 里 $a \geqslant b$.

証 如果格 L 到格 L' 内的一个映照 $a \rightarrow a'$ 能使从 $a \geqslant b$ 推

---

1) 这样記法在代数应用上比起通常先写較小的端点更为方便. ——著者注.

得 $a' \geqslant b'$，則这样的映照叫做保序映照．如果 $a \to a'$ 是一个同构，并且 $a \geqslant b$，則 $a \cup b = a$．于是，$a' \cup b' = a'$，从而 $a' \geqslant b'$．故 $a \to a'$ 是保序映照．逆映照 $a' \to a$ 显然也是保序的．反过来，設 $a \to a'$ 是 L 到 L' 上的一个 1—1 保序映照，并且它的逆映照也是保序的．令 $d = a \cup b$，則 $d \geqslant a, b$．于是，$d' \geqslant a', b'$．令 e' 是 L' 里使 $e' \geqslant a', b'$ 的任一个元素，并令元素 e 是 e' 在 L 里的象，則 $e \geqslant a, b$．于是，$e \geqslant d$；从而 $e' \geqslant d'$．这証明了 $d' = a' \cup b'$．同理可証 $(a \cap b)' = a' \cap b'$．

如果半序集合里一个元素 1 对于这集合里每个 a 有 $1 \geqslant a$，則 1 叫做全元素（单位，恆等元素）．从对偶方面說，如果一个元素 0 对于每个 a 有 $0 \leqslant a$，則 0 叫做零元素．如果半序集合里存在有这些元素，显然它們是唯一的．

习　題　70

1．求証：任一个羣的不变子羣的集合及（关于任一个算子集合 M 的）M-子羣的集合都是这个羣的子羣构成的格的子格．

2．令 S 表习題 69 的第 2 題里的半序集合．求恰当地定义 $f \cup g$ 及 $f \cap g$，并証：S 对于这些合成及給定的半序关系构成一个格．S 成一个完全格嗎？

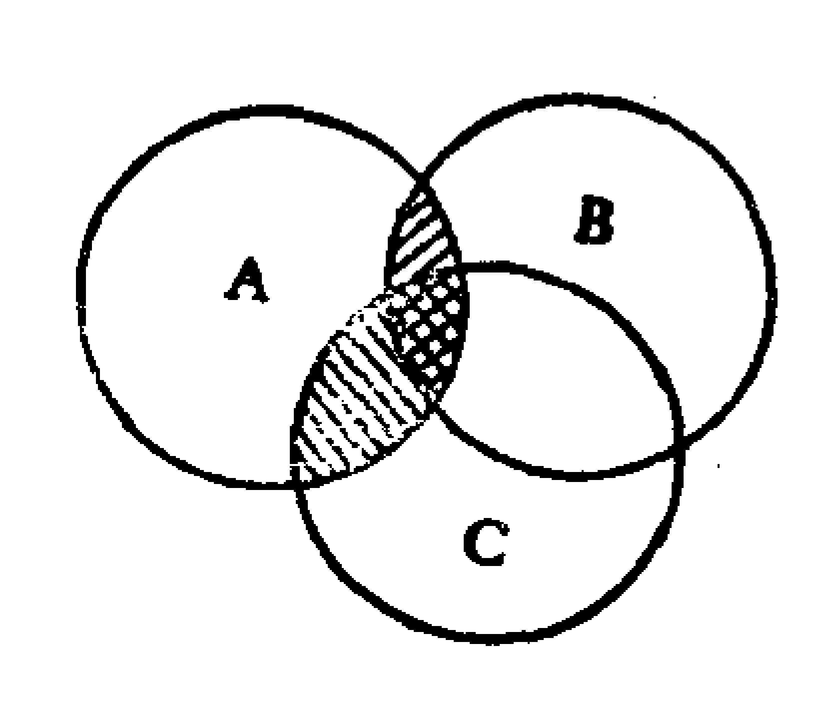
3．求証：任一个完全格有一个零元素及一个全元素．

4．如果带有一个全元素的一个半序集合里每个非空子集合有一个 g. l. b.，求証：这个半序集合是一个完全格．

3. 模格　格的两种合成里的一个，例如 $\cup$，可看作类似于环的加法，而另一个可看作类似于乘法．因此自然地引向分配格的論究，亦即

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c) \tag{1}$$

成立的格的論究．这种格的重要例子是存在的．例如，一个集合的所有子集合构成的格关于通常集合論上的和及交是可分配的；这可由左列图形显出，并且一般状况也是容易証明的．分配格的另一个例是正整数的格，



这里 $a \geqslant b$ 的意义是 $a | b$，而 $a \cup b$ 是 a 与 b 的 g. c. d. (a, b)，$a \cap b$ 是 a 与 b 的 l. c. m. $[a, b]$．于是，(1) 說明

$$[a, (b, c)] = ([a, b], [a, c]).$$

这結果容易由 (a, b) 及 $[a, b]$ 的性质得到証明（习题 47 的第 2 題）.

在任一个格里显然有 $a\cap(b\cup c)\geqslant a\cap b$ 及 $a\cap(b\cup c)\geqslant a\cap c$. 故

$$a\cap(b\cup c)\geqslant(a\cap b)\cup(a\cap c)$$

总是成立. 因此,要建立分配性,只須証明倒轉的不等式

$$a\cap(b\cup c)\leqslant(a\cap b)\cup(a\cap c)$$

也成立就可以了. 我們还知道,条件 (1) 是与对偶条件

$$(1') \qquad a\cup(b\cap c)=(a\cup b)\cap(a\cup c)$$

等价的. 这因为,如果 (1) 成立,则

$$\begin{aligned}(a\cup b)\cap(a\cup c) &= ((a\cup b)\cap a)\cup((a\cup b)\cap c)\\ &= a\cup((a\cup b)\cap c)\\ &= a\cup((a\cap c)\cup(b\cap c))\\ &= (a\cup(a\cap c))\cup(b\cap c)=a\cup(b\cap c).\end{aligned}$$

从对偶性,也可由 (1′) 推得 (1). 所以 (1) 的假設等价于 (1) 及 (1′) 的假設. 故对偶原理对于分配格显然也成立.

出現于代数上最重要的格（例如,环的理想构成的格）不是可分配的,但其中有若干个都适合比 (1) 較弱的形式,亦即

L_5. 如果 $a\geqslant b$, 則 $a\cap(b\cup c)=b\cup(a\cap c)$.

因为 $b=a\cap b$, 所以右端可用 $(a\cap b)\cup(a\cap c)$ 代替. 故在三个元素 a, b, c 有 $a\geqslant b$ 时,这个假設就得出分配律. 今述下面重要的定义.

定义 3. 如果一个格适合条件 L_5, 这种格叫做模格（狄得京格）. 这种格对于代数上其他分支的重要性基于下面的定理.

定理 2. 任一个羣的不变子羣構成的格是模格.

証 令 $\mathfrak{G}$ 是給定的羣,并令 $\mathfrak{H}_1,\mathfrak{H}_2,\mathfrak{H}_3$ 是不变子羣,其中 $\mathfrak{H}_1\geqslant\mathfrak{H}_2\ (\mathfrak{H}_1\supseteq\mathfrak{H}_2)$. 先就交 $\mathfrak{H}_1\cap(\mathfrak{H}_2\cup\mathfrak{H}_3)$ 来說, 这里 $\mathfrak{H}_2\cup\mathfrak{H}_3$ 現在是表示子羣构成的格里 $\mathfrak{H}_2$ 与 $\mathfrak{H}_3$ 的 l. u. b., 故 $\mathfrak{H}_2\cup\mathfrak{H}_3$ 是由 $\mathfrak{H}_2$ 与 $\mathfrak{H}_3$ 生成的子羣. 因为 $\mathfrak{H}_i$ 是不变子羣, 故 $\mathfrak{H}_2\cup\mathfrak{H}_3=\mathfrak{H}_2\mathfrak{H}_3=\mathfrak{H}_3\mathfrak{H}_2$. 于

是，如果 $a\in\mathfrak{H}_1\cap(\mathfrak{H}_2\cup\mathfrak{H}_3)$，則 $a=h_1\in\mathfrak{H}_1$，并且 $a=h_2h_3$，这里 $h_2\in\mathfrak{H}_2$ 而 $h_3\in\mathfrak{H}_3$. 由 $h_1=h_2h_3$ 得 $h_2^{-1}h_1=h_3$. 因为 $\mathfrak{H}_1\geqslant\mathfrak{H}_2$，故这个方程的左端表示 $\mathfrak{H}_1$ 的一个元素. 于是，$h_3\in\mathfrak{H}_1$；从而 $h_3\in\mathfrak{H}_1\cap\mathfrak{H}_3$. 这就証明了主要的不等式

$$\mathfrak{H}_1\cap(\mathfrak{H}_2\cup\mathfrak{H}_3)\leqslant\mathfrak{H}_2\cup(\mathfrak{H}_1\cap\mathfrak{H}_3).$$

前此已經說过，倒轉不等式是一般格理論上性質，故有

$$\mathfrak{H}_1\cap(\mathfrak{H}_2\cup\mathfrak{H}_3)=\mathfrak{H}_2\cup(\mathfrak{H}_1\cap\mathfrak{H}_3),$$

而定理完全証明.

模格的任一个子格显然是模格. 故任一个 M-羣的不变 M-子羣构成的格是模格. 于是，任一个模的子模构成的格及任一个环的(左、右、双側)理想构成的格都是模格. 但一个羣的所有子羣构成的格通常不是模格. 由于这种事实使我們难于把羣論完全包括于格論里面[1].

对偶原理在模格里是成立的. 这因为，L_5 的对偶命題是：如果 $a\leqslant b$，則 $a\cup(b\cap c)=b\cap(a\cup c)$，这与 L_5 說的是同一个事情. 模格的另一个有用的定义可由下面的定理引出.

定理 3. 格 L 是模格必須而且只須从 $a\geqslant b$ 及对于任一个 c 有 $a\cup c=b\cup c$，$a\cap c=b\cap c$ 时可推得 $a=b$.

証 令 L 是模格，并令 a,b,c 是 L 的元素，而有 $a\geqslant b$ 及 $a\cup c=b\cup c$，$a\cap c=b\cap c$. 則

$$a=a\cap(a\cup c)=a\cap(b\cup c)=b\cup(a\cap c)=b\cup(b\cap c)=b.$$

反过来，設 L 是适合定理里条件的任一个格. 令 $a\geqslant b$，則我們知道 $a\cap(b\cup c)\geqslant b\cup(a\cap c)$. 还有

$$(a\cap(b\cup c))\cap c=a\cap((b\cup c)\cap c)=a\cap c$$

及

$$a\cap c=(a\cap c)\cap c\leqslant(b\cup(a\cap c))\cap c\leqslant a\cap c,$$

故

$$(b\cup(a\cap c))\cap c=a\cap c.$$

---

1) 参看§4末段关于約当-霍尔德定理的說明. ——著者注.

由对偶性得

$$(a\cap(b\cup c))\cup c = b\cup c,$$
$$(b\cup(a\cap c))\cup c = b\cup c.$$

于是，

$$a\cap(b\cup c) = b\cup(a\cap c),$$

而 L 是模格.

今对于模格建立与羣的第二同构定理相类似的定理，即

定理 4. 如果 a 及 b 是一个模格里任意两个元素，则区间 $I[a\cup b, a]$ 与 $I[b, a\cap b]$ 同構.

証　令 x 属于区間 $I[a\cup b, a]$，则 $a\cup b\geqslant x\geqslant a$. 于是，$b\geqslant x\cap b\geqslant a\cap b$，而 $x\cap b$ 属于区間 $I[b, a\cap b]$. 同理，如果 y 属于 $I[b, a\cap b]$，則 $y\cup a$ 属于 $I[a\cup b, a]$. 故有 $I[a\cup b, a]$ 到 $I[b, a\cap b]$ 內的一个映照 $x\to x\cap b$ 及 $I[b, a\cap b]$ 到 $I[a\cup b, a]$ 內的一个映照 $y\to y\cup a$. 我們今来証明：它們是互相逆的，因而每个映照定义了从一个区間到另一个区間上的一个 1—1 对应. 这因为，令 $x\in I[a\cup b, a]$，由于 $x\geqslant a$，故

$$(x\cap b)\cup a = x\cap(a\cup b).$$

又因为 $x\leqslant a\cup b$，故得 $(x\cap b)\cup a = x$. 由对偶性可証：如果 $y\in I[b, a\cup b]$，則 $(y\cup a)\cap b = y$. 这証明了上面的論断. 因为这两个映照显然是保序的，故它們是格同构.

由这个定理使我們导出比同构概念更強的关于区間等价的概念. 首先，設有区間 $I[u, v]$ 及 $I[w, t]$，如果 L 里存在有元素 a, b 使所給的一对区間中的一个能表成 $I[a\cup b, a]$，而另一个有 $I[b, a\cap b]$ 形状，則我們称 $I[u, v]$ 与 $I[w, t]$ 是**轉置**(**相似**)**的**. 如果有一个有限序列

$$I[u, v] = I[u_1, v_1], I[u_2, v_2], \cdots, I[u_n, v_n] = I[w, t]$$

存在，从 $I[u, v]$ 开始，到 $I[w, t]$ 終止，使接連各对都是轉置，則区間 $I[u, v]$ 及 $I[w, t]$ 叫做**射影的**. 由此立知，我們所定义的关系是一种等价关系. 又由定理 4 知，射影区間是同构的.

今来观察在任一个 M-羣 $\mathfrak{G}$ 的不变 M-子羣所构成的格里，从

一对区間 $I[\mathfrak{H}, \mathfrak{K}]$, $I[\mathfrak{M}, \mathfrak{N}]$ 的射影性可推得商羣 $\mathfrak{H}/\mathfrak{K}$, $\mathfrak{M}/\mathfrak{N}$ 的 M-同构. 这只要考究一对轉置区間, 譬如說 $I[\mathfrak{H}_1 \cup \mathfrak{H}_2, \mathfrak{H}_1]$ 及 $I[\mathfrak{H}_2, \mathfrak{H}_1 \cap \mathfrak{H}_2]$ 就够了. 对于这两个区間, $(\mathfrak{H}_1 \cup \mathfrak{H}_2)/\mathfrak{H}_1$ 及 $\mathfrak{H}_2/(\mathfrak{H}_1 \cap \mathfrak{H}_2)$ 的同构可直接由羣的第二同构定理得出. 这个說明使我們可把一些格論上結果轉变为羣同构上結果.

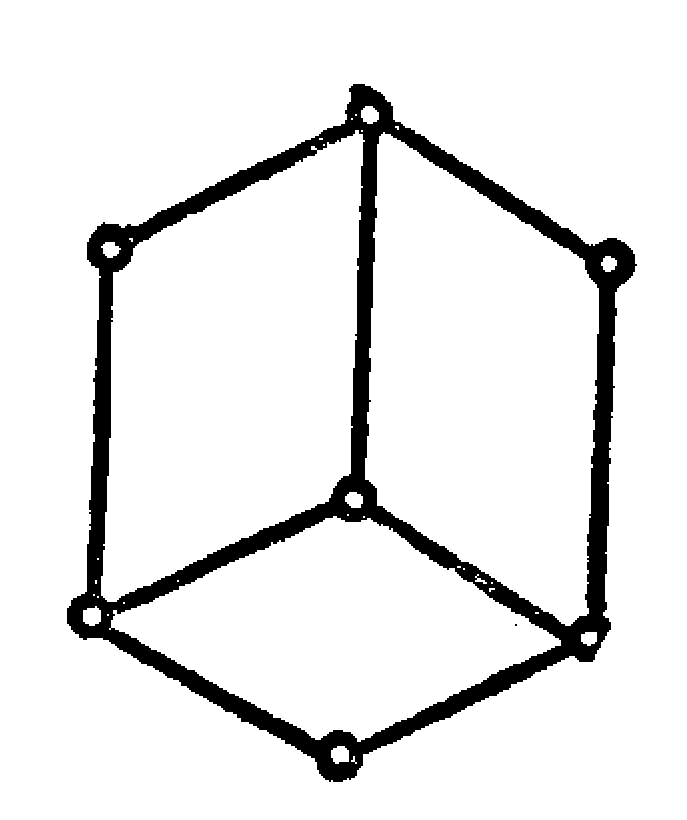
习　題　71

1. 如果一个格不是分配的, 求証: 它有一个 5 阶子格, 其图解是 §1 里第 1 图或第 2 图; 并証明: 一个非模格含有一个子格, 其图解是 §1 里第 1 图.

2. 求証: A_4 的子羣构成的格不是模格.

3. 如果 $\mathfrak{G}$ 是一个羣, 由两个元素 a 及 b 生成, 而 a 及 b 适合 $a^{p^m} = 1$, $b^{p^r} = 1$, $b^{-1}ab = a^n$, 这里 $n^{p^r} \equiv 1 \pmod{p^m}$, 求証: $\mathfrak{G}$ 的任意两个子羣可交换. 应用这結果求証: $\mathfrak{G}$ 的子羣构成的格是模格.

4. 如果在一个模格 L 里, a 复盖 $a \cap b$. 求証: $a \cup b$ 复盖 b. 具有这个性质的格叫做半模格. 驗証: 具有下面图解的格是半模格, 但不是模格.



4. 叔萊尔定理. 鏈条件　令 a 及 b 是一个模格里两个元素, 适合 $a \geqslant b$. 今考究联結 a 与 b 的有限降鏈

$$a = a_1 \geqslant a_2 \geqslant a_3 \geqslant \cdots \geqslant a_{n+1} = b. \tag{2}$$

如果一个这样鏈的項含有另一个鏈的所有項, 則說这个鏈是另一个鏈的一个加細. 如果在两个鏈的区間 $I[a_i, a_{i+1}]$ 間能建立一个 1—1 对应, 使对应区間是射影的, 則說这两个鏈成等价. 今用这些术語来叙述与羣論上叔萊尔定理相类似的結果, 但它的証明需要先証与札森豪斯引理(第三同构定理)相类似的下面引理:

引理. 令 a_1, a_1', a_2, a_2' 是一个模格的元素, 适合 $a_1 \geqslant a_1'$, $a_2 \geqslant a_2'$, 則下列三个区間

$$I[(a_1 \cap a_2) \cup a_1',\ (a_1 \cap a_2') \cup a_1'],$$

$$I[a_1\cap a_2,\ (a_1'\cap a_2)\cup(a_1\cap a_2')],$$
$$I[(a_1\cap a_2)\cup a_2',\ (a_1'\cap a_2)\cup a_2']$$

都是射影区間.

証 因为第二个区間对于下标 1 及 2 对称，并且第三个区間是由互換第一个区間里的下标 1 及 2 而得，故只要証明第一及第二个区間是射影的就够了. 令命

$$a = a_1\cap a_2,\quad b = (a_1\cap a_2')\cup a_1'.$$

則

$$a\cup b = (a_1\cap a_2)\cup(a_1\cap a_2')\cup a_1' = (a_1\cap a_2)\cup a_1',$$

并且

$$\begin{aligned} a\cap b &= (a_1\cap a_2)\cap((a_1\cap a_2')\cup a_1') \\ &= (a_1\cap a_2')\cup((a_1\cap a_2)\cap a_1') \\ &= (a_1\cap a_2')\cup(a_1'\cap a_2). \end{aligned}$$

这証明：第一个区間的形状为 $I[a\cup b,\ b]$，而第二个区間的形状为 $I[a,\ a\cap b]$. 故这两个区間是射影的.

定理 5. 联結一个模格里元素 $a, b (a\geqslant b)$ 的任意两个有限降鏈有等价的加細[1].

証 令命

(3) $$a = a_1\geqslant a_2\geqslant\cdots\geqslant a_{s+1} = b,$$

(4) $$a = b_1\geqslant b_2\geqslant\cdots\geqslant b_{t+1} = b$$

是联結 a 及 b 的两个降鏈. 仿照羣的情形导入元素

$$a_{ik} = (a_i\cap b_k)\cup a_{i+1}\quad (k = 1, 2, \cdots, t+1),$$
$$b_{ki} = (a_i\cap b_k)\cup b_{k+1}\quad (i = 1, 2, \cdots, s+1).$$

則

(5) $$a = a_{11}\geqslant a_{12}\geqslant\cdots\geqslant a_{1,t+1} = a_{21}\geqslant a_{22}\geqslant\cdots \geqslant a_{2,t+1}\geqslant\cdots\geqslant\cdots\geqslant a_{s,t+1} = b,$$

(6) $$a = b_{11}\geqslant b_{12}\geqslant\cdots\geqslant b_{1,s+1} = b_{21}\geqslant b_{22}\geqslant\cdots \geqslant b_{2,s+1}\geqslant\cdots\geqslant\cdots\geqslant b_{t,s+1} = b$$

---

1) 这里采用奥尔关于这个定理的表达. ——著者注.

分别是 (3) 及 (4) 的加細. 由引理知，$I[a_{ik}, a_{i,k+1}]$ 及 $I[b_{ki}, b_{k,i+1}]$ 是射影的；故可用对应 $I[a_{ik}, a_{i,k+1}] \to I[b_{ki}, b_{k,i+1}]$ 来証明定理 5.

上面証明的加細定理可用以导出关于模格的約当-霍尔德定理. 我們先来定义联結 $a, b(a > b)$ 的合成鏈为：一个有限序列

$$a = a_1 > a_2 > a_3 > \cdots > a_{n+1} = b,$$

其中每个 a_i 是 a_{i+1} 的一个复蓋. 仿照羣的情形，我們可直接建立下面的約当-霍尔德定理.

定理 6. 如果 $a = a_1 > a_2 > \cdots > a_{n+1} = b$ 及 $a = a_1' > a_2' > \cdots > a_{m+1}' = b$ 是联結模格 L 里 a 及 b 的两个合成鏈，则 $n = m$，並且在区間 $I[a_i, a_{i+1}]$，$I[a_j', a_{j+1}']$ 間存在有一个 1—1 对应，使对应的区間是射影的.

为簡单計，今假設 L 含有 0 及 1，并在前面討論里取 $a = 1$，$b = 0$. 于是，如果有联結 1 及 0 的一个合成鏈存在，則說 L 有有限长. 这鏈里由 L 唯一决定的区間个数叫做 L 的长(維).

仿照羣的情形(第五章的 §8)易証：带 0 及 1 的一个模格有有限长，必須而且只須下面的两个鏈条件成立.

降鏈条件. L 里不存在无限眞降鏈 $a_1 > a_2 > a_3 > \cdots$.

升鏈条件. L 里不存在无限眞升鏈 $a_1 < a_2 < a_3 < \cdots$.

今設 L 是带 0, 1 的模格，并設 L 有有限长. 如果 a 是 L 的一个元素，則由 $\leqslant a$ 的元素 x 构成的子格 L_a 也适合賦予 L 的各条件. 显然，a 是 L_a 的全元素. L_a 的长我們叫做 a 的秩(維数)，記作 $l(a)$. 如果 $a \geqslant b$，則显然有

$$l(a) = l(b) + I[a, b] \text{ 的长}$$

故对于 L 里任意 a 及 b 有

$$l(a \cup b) = l(a) + I[a \cup b, a] \text{ 的长},$$
$$l(b) = l(a \cap b) + I[b, a \cap b] \text{ 的长}.$$

因为 $I[a \cup b, a]$ 与 $I[b, a \cap b]$ 同构，故它們的长相等. 于是，

$$l(a \cup b) - l(a) = l(b) - l(a \cap b),$$

或

$$(7) \qquad l(a\cup b)=l(a)+l(b)-l(a\cap b).$$

这公式叫做模格的基本維数关系.

本节的結果重新得到关于任一个 M-羣 $\mathfrak{G}$ 的不变 M-子羣的叔萊尔定理及約当-霍尔德定理. 由鏈的区間所决定商羣的同构可由这些区間的射影性来保証. 例如, 我們可由格的結果容易引出关于主合成羣列及关于特征羣列的約当-霍尔德定理. 另一方面, 因为一个羣的所有子羣构成的格不必是模格, 所以我們給出的格的定理不能用于通常的合成羣列. 我們需要更复杂的概念以得通常合成羣列的理論[1].

习 題 72

1. 設 A 是格 L 的一个子集合, 如果 (1) $a, b\in A$ 可推得 $a\cap b\in A$, 并且 (2) $a\in A$ 及 $x\in L$ 可推得 $a\cup x\in A$, 則說 A 是一个理想. 如果对于固定的 $a\in L$, A 由能使 $x\geqslant a$ 的所有 $x\in L$ 构成, 則 A 叫做一个主理想, 記作 (a). 求証: L 适合降鏈条件必須而且只須 L 的每个理想是主理想.

一个理想的对偶叫做对偶理想. 試述对偶理想的定义, 及上面結果的对偶性質.

5. 带升鏈条件格的分解論 我們今考究諾德环里一部分理想理論的格抽象. 設 L 是适合升鏈条件的模格. 仿照理想的特殊情形, 如果 L 里一个元素 $a=a_1\cap a_2$, 这里 $a_i>a$, 則說 a 是(交)可約元素. 我們易証 (例如, 用类似于因子归納法原理)[2]: L 的任一个元素可以有限个不可約元素的 g. l. b. 表出.

准素理想的理論不能轉移于格. 故必須以不可約性概念来专門处理; 并且按唯一性所能建立的結果只是比較弱的結果, 即: 用不可約元素的 g. l. b. 作的任意两个无贅分解里, 項数是唯一的. 如果 $a=q_1\cap q_2\cap\cdots\cap q_m$, 并且 $q_1\cap\cdots\cup q_{i-1}\cap q_{i+1}\cap\cdots\cap q_m>a$ $(i=1, 2, \cdots, m)$, 我們与前面一样叫表示 $a=q_1\cap q_2\cap\cdots\cap q_m$

1) 参看柏克霍夫 (G. Birkhoff) 著的"格論" (Lattice theory) 增訂版 (1951), 87—89 頁, 及 89 頁上的文献. ——著者注.

2) 因子归納法原理是說: 設环 $\mathfrak{R}$ 适合升鏈条件; 如果一个性質 E 对于 $\mathfrak{R}$ 里每个理想 $\mathfrak{A}$ 的所有眞因子——如果理想 $\mathfrak{B}\supset\mathfrak{A}$, 則說 $\mathfrak{B}$ 是 $\mathfrak{A}$ 的眞因子——都成立, 則性質 E 对于 $\mathfrak{A}$ (特别是对于单位理想, 亦即对于含有 $\mathfrak{R}$ 的所有元的理想) 也成立. ——譯者註.

做无贅表示.

今設 a 有任意两种表示(不一定是无贅的):

(8) $$a = q_1 \cap q_2 \cap \cdots \cap q_m = r_1 \cap r_2 \cap \cdots \cap r_n,$$

这里 q_i 及 r_j 是不可約的. 我們要証: 任一个 q_i 可用一个适宜的 $r_{i'}$ 来代替,使得 a 还可表示如

$$a = q_1 \cap \cdots \cap q_{i-1} \cap r_{i'} \cap q_{i+1} \cap \cdots \cap q_m.$$

这只要取 $i = 1$ 时証明就够了. 今引入記法

$$r_j' = r_j \cap q_2 \cap \cdots \cap q_m \quad (j = 1, 2, \cdots, n),$$

則有 $a = r_1' \cap r_2' \cap \cdots \cap r_n'$ 并且 $r_i' \leqslant q_2 \cap q_3 \cap \cdots \cap q_m$. 因为区間

(9) $$I[q_2 \cap \cdots \cap q_m, a] = I[q_2 \cap \cdots \cap q_m, q_1 \cap q_2 \cap \cdots \cap q_m]$$

与

(10) $$I[q_1 \cup (q_2 \cap \cdots \cap q_m), q_1]$$

同构,而 q_1 在 (10) 里是不可約的,故 a 在 (9) 里是不可約的. 但分解式 $a = r_1' \cap r_2' \cap \cdots \cap r_n'$ 在 (9)里成立,故对于适宜的 i, $q_1 = r_{i'}'$. 这証明了下面的定理.

定理 7. 如果 $a = q_1 \cap q_2 \cap \cdots \cap q_m = r_1 \cap r_2 \cap \cdots \cap r_n$ 是模格里一个元素用不可約元素的 g. l. b. 作出的两个表示, 則对于每个 q_i 存在有一个 $r_{i'}$ 使 $a = q_1 \cap \cdots \cap q_{i-1} \cap r_{i'} \cap q_{i+1} \cap \cdots \cap q_m$.

这結果的簡单推論是唯一性定理:

定理 8. 一个元素用不可約元素的 g. l. b. 作出的任意两个无贅表示的項数相同.

証 应用定理 7 ,我們可写

(11) $$a = r_{1'} \cap q_2 \cap \cdots \cap q_m = r_{1'} \cap r_{2'} \cap q_3 \cap \cdots \cap q_m = \cdots = r_{1'} \cap r_{2'} \cap \cdots \cap r_{m'}$$ [1].

因为分解式 $a = r_1 \cap r_2 \cap \cdots \cap r_n$ 是无贅的,故所有 r_i 出現于 (11) 的末行里. 于是, $m \geqslant n$. 由对称性得 $m = n$.

6. 无关性 設 L 是带 0 及 1 的模格. 如果 L 的一个有限集合 $a_1, a_2, \cdots, a_n$ 适合

(12) $$a_i \cap (a_1 \cup \cdots \cup a_{i-1} \cup a_{i+1} \cup \cdots \cup a_n) = 0$$

---

1) 这里 2′, 3′, … 与定理 7 里所用的記号,意义上稍有不同. ——著者注.

$$(i=1,2,\cdots,n),$$

则这个集合叫做(联合)无关的．前此在羣的直接积理論里已遇到这个概念．本节(主要在习題里)将指出一部分直接积理論如何轉移于格．这里我們要导出的主要結果是下面的定理．

定理 9. 如果元素 $a_1, a_2, \cdots, a_n$ 是无关的，则

(13) $$(a_1\cup\cdots\cup a_r\cup a_{r+1}\cup\cdots\cup a_s)\cap(a_1\cup\cdots\cup a_r\cup a_{s+1}\cup\cdots\cup a_t)=a_1\cup\cdots\cup a_r.$$

証　先証

(14) $$(a_1\cup\cdots\cup a_s)\cap(a_{s+1}\cup\cdots\cup a_n)=0.$$

当 $s=1$ 时，由假設知它是成立的．次設 (14) 在 $s-1$ 时成立；于是，由模性及归納法假設，得

$$\begin{aligned}&(a_1\cup\cdots\cup a_s)\cap(a_{s+1}\cup\cdots\cup a_n)\\ \leqslant\ &(a_1\cup\cdots\cup a_s)\cap(a_s\cup a_{s+1}\cup\cdots\cup a_n)\\ =\ &((a_1\cup\cdots\cup a_{s-1})\cap(a_s\cup\cdots\cup a_n))\cup a_s=a_s.\end{aligned}$$

因为 $a_s\cap(a_{s+1}\cup\cdots\cup a_n)=0$，故

$$\begin{aligned}&(a_1\cup\cdots\cup a_s)\cap(a_{s+1}\cup\cdots\cup a_n)\\ =\ &(a_1\cup\cdots\cup a_s)\cap(a_{s+1}\cup\cdots\cup a_n)\cap a_s=0.\end{aligned}$$

由此可見，(14)对于所有 s 都成立．故我們可应用模性假設于(13)的左端以得右端．

由 (13) 可得若干有用的推論，其中一些見于下面的习題里．

习　題　73

1. 如果 $a_1, a_2, \cdots, a_n$ 是一个无关集合，求証：任一个子集合是无关的；并証明：元素

$$b_1=a_1\cup\cdots\cup a_{r_1},\quad b_2=a_{r_1+1}\cup\cdots\cup a_{r_2},\cdots,b_k=a_{r_{k-1}+1}\cup\cdots\cup a_{r_k}$$

是无关元素，这里 $r_1<r_2<\cdots<r_k=n$．

2. 令 $a_1, a_2, \cdots, a_n$ 是无关元素的一个集合，且有 $a_1\cup a_2\cup\cdots\cup a_n=1$．定义

$$b_i=a_1\cup\cdots\cup a_{i-1}\cup a_{i+1}\cup\cdots\cup a_n.$$

求証对偶关系：

$$\begin{gathered}b_i\cup(b_1\cap\cdots\cap b_{i-1}\cap b_{i+1}\cap\cdots\cap b_n)=1,\\ b_1\cap b_2\cap\cdots\cap b_n=0,\\ a_i=b_1\cap\cdots\cap b_{i-1}\cap b_{i+1}\cap\cdots\cap b_n.\end{gathered}$$

3. 如果元素 $a_1, a_2, \cdots, a_n$ 是无关的，并且 $(a_1\cup\cdots\cup a_n)\cap a_{n+1}=0$，求証：元素 $a_1、a_2、\cdots, a_{n+1}$ 是无关的．求証：集合 $a_1, a_2, \cdots, a_n$ 是无关的必須而且只須 $(a_1\cup\cdots$

$\cup a_i) \cap a_{i+1} = 0$ $(i = 1, 2, \cdots, n-1)$.

4. 如果L适合鏈条件，求証：元素 $a_1, a_2, \cdots, a_n$ 是无关的必須而且只須

$$l(a_1 \cup a_2 \cup \cdots \cup a_n) = l(a_1) + l(a_2) + \cdots + l(a_n).$$

如果一个元素 $a = a_1 \cup a_2$，这里 a_i 是无关的，并且 $\neq a$，则說 a 是(联合)可分解的. 如果L适合降鏈条件，则仿照羣的情形所用的論点(第五章的 §12 末段)可証：L的任一个元素可用有限个无关的而且不可分解的元素的 l. u. b. 来表示.

如果 $a = b \cup c = b \cup d$，这里 $b \cap c = 0 = b \cap d$，则区間 $I[a, b]$ 及 $I[c, 0]$ 与区間 $I[a, b]$ 及 $I[d, 0]$ 是轉置. 于是，$I[c, 0]$ 及 $I[d, 0]$ 是射影的. 所以，如果L里存在有 b，使

$$b \cup c = b \cup d, \quad b \cap c = b \cap d = 0,$$

则說元素 c 及 d 是直接射影的. 这个概念被用于把克魯尔-叔密特定理扩张到格論上. 本书只述这个結果，而不附証明.

定理. 令L是带 0 及 1 的一个模格，适合降鏈及升鏈条件. 設

$$a = a_1 \cup a_2 \cup \cdots \cup a_m = b_1 \cup b_2 \cup \cdots \cup b_n,$$

这里 a_i 及 b_j 都是无关的並且不可分解的元素，则 $m = n$，並且 a_i 与 b_j 可列成 1—1 对应，使对应元素是直接射影的.

这个定理由庫洛什 (Курош) 及奥尔发現[1]. 由此立可推得关于羣的克魯尔-叔密特定理，只除了涉及中間分解的叙述的部分.

7. 有余模格

定义 4. 如果带 0 及 1 的格对于L里每个 a 都存在一个 a' 使 $a \cup a' = 1$, $a \cap a' = 0$，则說L是有余格.

如果 a 是带 0 及 1 的格里任一个元素，而元素 a' 能使 $a \cup a' = 1$, $a \cap a' = 0$，则 a' 叫做 a 的余元素. 故由上面的定义知，一个格是有余的必須而且只須L里每个 a 都有一个余元素. 如果 $b \leqslant a$，则使 $b \cup b_1 = a$ 及 $b \cap b_1 = 0$ 的元素 $b_1 (\leqslant a)$ 叫做 b 关于 a 的余元素.

一个集合的子集合构成的格是有余格. 一个子集合 A 的余元

---

1)参看柏克霍夫著的"格論"，增訂版，94 頁. ——著者注.

素是通常集合論上的余子集合，亦即所有元素 $a' \notin A$ 的集合 A'. 如果一个有限交换羣的所有元素的阶是有限素数，則羣的子羣构成的格是有余格. 这可由現在即将建立的判别准則得出.

令 L 是一个有余模格，并令 a 及 b 是 L 的任意两个元素，而 $b \leqslant a$, 則有一个元素 b' 存在,使 $b \cup b' = 1, b \cap b' = 0$. 故由模性，有

$$a = a \cap (b \cup b') = b \cup (a \cap b') = b \cup b_1,$$

这里 $b_1 = a \cap b'$. 因为 $b \cap b_1 = b \cap a \cap b' = 0$, 显然 b_1 是 b 关于 a 的余元素. 故知,如果 L 是模格，并且是有余格，則对于 L 里任一个 a, 任一个 $b(\leqslant a)$ 关于 a 的余元素都存在. 另一种說法是: 对于 L 里每个 a, 元素 $\leqslant a$ 的子格 L_a 是有余格.

在有余格理論里，点的概念极为重要. 如果带 0 的格里一个元素 p 是 0 的一个复盖,則 p 叫做一点. 如果 L 适合降鏈条件,則 L 含有点. 这因为,我們可选一个 $a_1 > 0$. 如果 a_1 不是 0 的复盖,則存在一个 a_2 使 $a_1 > a_2 > 0$. 如果 a_2 不是一点，則有 a_3 存在使 $a_1 > a_2 > a_3 > 0$. 由降鏈条件知，这个方法进行有限次后必将停止下来,而达到 L 里一点.

今設 L 是有余格,并适合降鏈及升鏈条件. 令 p_1 是 L 里一点，并令 p_1' 是 p_1 的一个余元素. 如果 $p_1' \neq 0$, 則对于 $L_{p_1'}$ 可使用降鏈条件以得一点 $p_2 \leqslant p_1'$. 因为 $p_1 \cap p_2 = 0$, 故 $(p_1 \cup p_2) > p_1$. 又因为 $p_1 \cup p_2$ 有一个余元素,如果它 $\neq 0$, 必含有一点 p_3. 于是，$(p_1 \cup p_2) \cap p_3 = 0$, 并且 $p_1 \cup p_2 \cup p_3 > p_1 \cup p_2$. 連續进行下去,得点 $p_1, p_2, p_3, \cdots$ 的一个序列,使

$$p_1 < p_1 \cup p_2 < p_1 \cup p_2 \cup p_3 < \cdots.$$

由升鏈条件知，經过有限次后，譬如說 $n(<\infty)$ 次后,就要終止. 当这情况出現时,可知 $p_1 \cup p_2 \cup \cdots \cup p_n$ 有 0 作为一个余元素. 这意味着 $1 = p_1 \cup p_2 \cup \cdots \cup p_n$. 故 1 是有限个点的一个 l. u. b. 不但如此,我們所选的 p_i 是使

$$(p_1 \cup p_2 \cup \cdots \cup p_i) \cap p_{i+1} = 0 \quad (i = 1, 2, \cdots, n-1).$$

所以,如果 L 是模格,則 p_i 是无关元素(习題 73 的第 3 題).

反过来說，設 L 是带 0 及 1 的任一个模格，它具有这样性質，即 1 是有限个点的一个 l. u. b.。今証：L 适合鏈条件，并且 L 是有余格。令 $1 = p_1 \cup p_2 \cup \cdots \cup p_n$，这里 p_i 是点。我們可設所用的記法是使 $p_1, p_2, \cdots, p_m$ 能为集合 $p_1, p_2, \cdots, p_n$ 的一个最大无关子集合。于是，我們可肯定 $1 = p_1 \cup p_2 \cup \cdots \cup p_m$；这因为，如果否定这結果，則必有一个 $i > m$ 存在，使 $p_i \nleq p_1 \cup p_2 \cup \cdots \cup p_m$。由此可推得

$$\bar{p}_i \equiv p_i \cap (p_1 \cup \cdots \cup p_m) < p_i;$$

于是，$\bar{p}_i = 0$。因而 $p_1, \cdots, p_m, p_i$ 是一个无关集合，这与 m 的极大性矛盾。故得 $1 = p_1 \cup p_2 \cup \cdots \cup p_m$。因为 p_j $(j \leqslant m)$ 是无关的，故

$$(p_1 \cup p_2 \cup \cdots \cup p_j) \cap p_{j+1} = 0 \quad (j = 1, 2, \cdots, m-1).$$

于是，区間 $I[p_1 \cup p_2 \cup \cdots \cup p_{j+1}, p_1 \cup p_2 \cup \cdots \cup p_j]$ 与 $I[p_{j+1}, 0]$ 是轉置；从而 $p_1 \cup p_2 \cup \cdots \cup p_{j+1}$ 是 $p_1 \cup p_2 \cup \cdots \cup p_j$ 的一个复盖。由此可見

$$1 = (p_1 \cup \cdots \cup p_m) > (p_1 \cup \cdots \cup p_{m-1}) > \cdots > p_1 > 0$$

是 L 的一个合成鏈。这样鏈的存在就可推得两个鏈条件。

次証 L 是有余格。令 $1 = p_1 \cup p_2 \cup \cdots \cup p_n$，这里 p_i 是点。如果 a 是 L 的任一个元素，并且 $a \neq 1$，我們可选一个 $p_{i_1} \nleq a$。于是，$a \cap p_{i_1} = 0$，并且 $a_1 = a \cup p_{i_1} > a$。如果 $a_1 \neq 1$，則可找到一个 p_{i_2}，使 $a_1 \cap p_{i_2} = 0$。由这个方法得出 p_j 的一个子集合 $p_{i_1}, p_{i_2}, \cdots, p_{i_r}$，使

$$a \cap p_{i_1} = 0,$$
$$(a \cup p_{i_1}) \cap p_{i_2} = 0, \cdots, (a \cup p_{i_1} \cup \cdots \cup p_{i_{r-1}}) \cap p_{i_r} = 0,$$
$$a \cup p_{i_1} \cup \cdots \cup p_{i_r} = 1.$$

由为首 r 个方程指出，集合 $a, p_{i_1}, \cdots, p_{i_r}$ 是无关的。故 $a \cap (p_{i_1} \cup \cdots \cup p_{i_r}) = 0$；而由最后方程知，$p_{i_1} \cup \cdots \cup p_{i_r}$ 是 a 的余元素。

今把主要結果綜結为下面的定理。

定理 10. 如果 L 是一个有余模格，适合升鏈及降鏈条件，則 L 的元素 1 是无关点的一个 l. u. b.。反过來，如果 L 是帶有 0 及 1

的一个模格，而 1 是有限个点的一个 l. u. b.，则 L 是有余格，並适合升鏈及降鏈条件.

在羣 $\mathfrak{G}$ 的子羣构成的格 $\mathfrak{L}$ 里，素数阶循环子羣是一点. 所以，如果 $\mathfrak{G}$ 是有限交换羣，并且 $\mathfrak{G}$ 的每个元素的阶数都是素数，则 $\mathfrak{L}$ 适合鏈条件，是一个模格，并且 $\mathfrak{L}$ 里的 1 是点的一个 l. u .b.。这証明了上面的 $\mathfrak{L}$ 是有余格的說法.

习　　题　74

1. 求証：对于一个有余模格，可从两个鏈条件中的任一个推得另一个.

8. 布尔代数

定义 5. 布尔代数是带有 0 及 1 的一个格，它是分配的，并且是有余的.

布尔代数最重要的例子是任一个集合 S 的子集合构成的格. 一般来說，S 的任一个子集合域是一个布尔代数；換句話說，子集合的任一个集合，如果对于 $\cup$ 及 $\cap$ 封閉，并且含有 $1(=S)$ 及 $0(=\emptyset)$，还含有这集合里任一个子集合的余集合时，这集合是一个布尔代数.

下面定理給出任一个布尔代数里余元素的最重要初等性質.

定理 11. 一个布尔代數 B 里任一个元素 a 的余元素 a' 是唯一决定的. 映照 $a\to a'$ 是 B 到它自身上的 1—1 对应；它的周期为 $2(a''=a)$，並且适合条件

$$(a\cup b)'=a'\cap b',\quad (a\cap b)'=a'\cup b'. \tag{15}$$

証　令 a 是 B 的任一个元素，并令 a' 及 a_1 是使 $a\cup a'=1$ 及 $a\cap a_1=0$ 的两个元素. 則

$$a_1=a_1\cap 1=a_1\cap(a\cup a')=(a_1\cap a)\cup(a_1\cap a')=a_1\cap a'.$$

所以，如果更有 $a\cup a_1=1$ 及 $a\cap a'=0$，則 $a'=a'\cap a_1$. 于是，$a'=a_1$. 这証明了余元素的唯一性. 至此，显然知 a 是 a' 的余元素. 故 $a''\equiv(a')'=a$. 这証明了映照 $a\to a'$ 的周期是 2. 因此，这映照是 B 到它自身上的 1—1 映照. 今令 $a\leqslant b$，則 $a\cap b'\leqslant b\cap b'=0$，而

$$b' = b' \cap 1 = b' \cap (a \cup a') = (b' \cap a) \cup (b' \cap a') = b' \cap a'.$$

故 $b' \leqslant a'$. 因为 $a \to a'$ 是 B 到它自身上的 1—1 对应，并且是逆序的（就是說，如果 $a \leqslant b$，則 $b' \leqslant a'$），故由使用証明定理 1 的論点可証 (15) 成立.

就历史上說来，布尔代数是格研究的开端. 布尔要使命題学形式化而导入这种代数. 长期以来都以为表示这些代数系的代数类型与含于熟悉的数系的代数类型在实质上完全不同，但实际上并非如此，相反地我們将要看到布尔代数的理論与环的一个特殊类的理論等价. 这个事实可基于任一个布尔代数可看作是一个环关于适宜定义的合成的結果而得出証明.

要从一个布尔代数 B 作出一个环，我們引入新的合成

$$a + b = (a \cap b') \cup (a' \cap b),$$

叫做 a 与 b 的**对称差**. 我們立知，$(a \cap b') \cup (a' \cap b) = (a \cup b) \cap (a \cap b)'$. 故在集合 S 的子集合的这一特殊情形，对称差 $U + V$ 恰是属于 U 与属于 V 但不同时属于这两个集合的元素的全体. 我們今将証明：B 关于合成 $+$ 作为加法及合成 $\cap$ 作为乘法成一个环. 今后并以通常所用环的乘法記法 ab 代替 $a \cap b$.

显然 $+$ 是可交换的. 要証結合性，首先有

$$(a + b)' = (a \cap b) \cup (a' \cap b').$$

于是，

$$\begin{aligned}(a + b) + c &= \{((a \cap b') \cup (a' \cap b)) \cap c'\} \\ &\quad \cup \{((a \cap b) \cup (a' \cap b')) \cap c\} \\ &= (a \cap b' \cap c') \cup (a' \cap b \cap c') \cup (a \cap b \cap c) \cup (a' \cap b' \cap c).\end{aligned}$$

这对于 a, b 及 c 是对称的，故在特款得 $(a + b) + c = (c + b) + a$. 因此，从交换性可推得結合律. 显然，

$$a + 0 = (a \cap 1) \cup (a' \cap 0) = a,$$

并且

$$a + a = (a \cap a') \cup (a' \cap a) = 0.$$

故 B 关于 $+$ 是一个交换羣.

我們知道，$\cdot$ $(= \cap)$ 是可結合的、故只須驗証分配律. 这可

由

$$
\begin{aligned}
(a+b)c &= ((a\cap b')\cup(a'\cap b))\cap c\\
&= (a\cap b'\cap c)\cup(a'\cap b\cap c),\\
ac+bc &= ((a\cap c)\cap(b\cap c)')\cup((a\cap c)'\cap(b\cap c))\\
&= ((a\cap c)\cap(b'\cup c'))\cup((a'\cup c')\cap(b\cap c))\\
&= (a\cap c\cap b')\cup(a'\cap b\cap c)
\end{aligned}
$$

得証. 故 $B,+,\cdot$ 是一个环.

环 $B,+,\cdot$ 还有下面各性質:这个环是可交換的,它有一个恆等元素,并且它的所有元素都是同勢元素. 所有这些性質都是带 1 的任一个格的合成 $\cap$ 的熟知性質. 我們还知道,B 的每个元素在它的加法羣里的阶是 $\leqslant 2$. 就环来說,这些性質并非无关的;这因为,如果环里每个元素 a 适合 $a^2=a$,則可推得 $2a=0$ 及对于每两个 a,b 有 $ab=ba$. 要証这些事实,須知

$$a+b+ab+ba=a^2+b^2+ab+ba=(a+b)^2=a+b.$$

故

$$ab+ba=0. \tag{16}$$

如果于 (16) 里令 $a=b$, 并应用 a 的同勢性,則得 $2a=0$; 于是, $a=-a$. 故由 (16) 得 $ab=ba$. 因此,关于 $B,+,\cdot$ 的主要事实是:它有一个恆等元素,并且它的所有元素都是同勢的. 故我們可导入下面的定义.

定义 6. 如果一个环的所有元素都是同勢的, 这个环叫做**布尔环**.

其次,我們要証:带恆等元素的任一个布尔环 $\mathfrak{B}$ 定义一个布尔代数. 为着把上面用的方法倒轉过来,今定义 $a\cup b=a+b-ab$, 及 $a\cap b=ab$. 我們知道(第二章的 §3), $\cup$(圓合成)是可結合的. L_1—L_4 里其他法則都可由上述关于 $\mathfrak{B}$ 的假設及交換性立刻导出故 $\mathfrak{B},\cup,\cap$ 是一个格. 因为

$$
\begin{aligned}
(a\cup b)\cap c &= (a+b-ab)c\\
&= ac+bc-abc\\
&= ac+bc-acbc
\end{aligned}
$$

$$= (a \cap c) \cup (b \cap c),$$

故这个格是分配格. 我們还易知, 1 及 0 分别是格的全元素及零元素, 并且 $a' = 1 - a$ 具有 a 的余元素的作用. 故 $\mathfrak{B}$ 是一个布尔代数.

最后要指出,我們所用的两个方法可以彼此逆推的. 譬如,假定从布尔代数 $B, \cup, \cap$ 出发,则得环 $B, +, \cdot$,这里 $a + b = (a \cap b') \cup (a' \cap b)$, $ab = a \cap b$. 用后一个方法于 $B, +, \cdot$, 給出合成 $a \bar{\cup} b \equiv a + b - ab$ 及 $a \bar{\cap} b = ab \equiv a \cap b$. 由于 $1 - a = 1 + a = (1 \cap a') \cup (1' \cap a) = a'$. 于是

$$a \bar{\cup} b = a + b - ab = 1 - (1 - a)(1 - b)$$
$$= (a' \cap b')' = a \cup b.$$

故合成 $\bar{\cup}$, $\bar{\cap}$ 与原来的 $\cup$, $\cap$ 重合. 反过来, 設从带 1 的布尔环出发, 并定义 $a \cup b = a + b - ab$, $a \cap b = ab$ 及 $a \oplus b = (a \cap b') \cup (a' \cap b)$, $a \odot b = a \cap b = ab$, 则 $a' = 1 - a$, 并且

$$\begin{aligned} a \oplus b &= (a \cap (1 - b)) \cup ((1 - a) \cap b) \\ &= a(1 - b) \cup (1 - a)b \\ &= (a - ab) \cup (b - ab) \\ &= a - ab + b - ab - (a - ab)(b - ab) \\ &= a - ab + b - ab - ab + ab + ab - ab \\ &= a + b. \end{aligned}$$

故 $\oplus$ 与 $+$ 重合, $\odot$ 与 $\cdot$ 重合. 这就完成了下面定理的証明:

定理 12. (斯敦(Stone)定理) 布尔代數与帶恆等元素的布尔环这兩类型的抽象代數系是等价的.

习　题　75

1. 求証: 任一个布尔代数关于两个合成 $a \oplus b = (a \cup b') \cap (a' \cup b)$, $a \odot b = a \cup b$ 定义一个环. 求証: $a \oplus b = 1 + a + b$, $a \odot b = a + b + ab$, 这里 $+$ 及 $\cdot$ 是按书中定义的合成.

2. 如果 e 及 f 是一个环的同势元素,并且 $ef = fe$. 証明: ef 及 $e + f - ef$ 是同势元素. 求証: 属于带恆等元素的任一个环的心的同势元素关于合成 $e \cup f = e + f - ef$, $e \cap f = ef$ 成一个布尔代数.

3. 如果对于任一个环存在一个素数 p, 使环里每个 a 适合 $pa = 0$ 及 $a^p = a$, 求証:这个环是交换环.

术 語 索 引

三 划

四 划

五　划

六　划

七　划

八 划

九 划

十 划

十 一 划

十 二 划

十 三 划

十 四 划

十 五 划

人 名 索 引

四 划

五 划

六 划

七 划

八 划

九 划

十 划

十 一 划

十 二 划

十 三 划

十 四 划

十 六 划

［Ｇｅｎｅｒａｌ Ｉｎｆｏｒｍａｔｉｏｎ］
书名＝抽象代数学　　卷１　　基本概念
作者＝Ｎ．贾柯勃逊
页数＝２００
ＳＳ号＝１０１００８６２
出版日期＝１９６０年０２月第１版